

ContractPodAi Data Processing Addendum

Last Modified: 10 November 2021a

What's New/Modified: Clarified § II(a)(i) regarding Personal Data and simplified the wording of § II(a) generally.
Noted in § III(a) that we will comply with applicable Data Protection Laws.
Added text in § III(f) that we will issue a certificate of deletion upon request.
Clarified § VIII(c) that our use of California Personal Information is strictly limited.

This ContractPod Data Processing Addendum (“DPA”) reflects the parties’ agreement with respect to the Processing of Personal Data by us (ContractPodAi) on behalf of you (our Customer) in connection with the agreement between you and us (“Agreement,” also referred to in this DPA as the “Master Terms”).

This DPA is supplemental to, and forms an integral part of, the Master Terms and is effective upon its incorporation into the Master Terms, which may be specified in the Master Terms, an Order, or an executed amendment to the Master Terms. If there is any conflict or inconsistency between the Master Terms or this DPA, the DPA will take precedence over the Master Terms to the extent of such conflict or inconsistency.

The term of this DPA will follow the term of your ContractPodAi order (typically set forth in your Order Form).

I. 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 or control of more than 50% of the voting interests of the subject entity.
- “**California Personal Information**” means Personal Data that is subject to the protection of the CCPA.
- “**CCPA**” means California Civil Code Sec. 1798.100 et seq., also known as the California Consumer Privacy Act of 2018.
- “**Consumer**”, “**Business**”, “**Sell**,” and “**Service Provider**” will have the meanings given to them in the CCPA.
- “**ContractPod USA**” will mean ContractPod Technologies Inc., a Delaware corporation with its primary business office in New York.
- “**Controller**” means the natural or legal person, public authority, agency, or other body, which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
- “**Data Protection Laws**” means the applicable legislation relating to data protection and privacy which applies to the respective party in the role of Processing Personal Data in question under the Master Terms, including without limitation European Data Protection Laws, the CCPA, and the data protection and privacy laws of Australia and Singapore; in each case as amended, repealed, consolidated, or replaced from time to time.
- “**Data Subject**” means the individual to whom Personal Data relates.
- “**Europe**” means the European Union, the European Economic Area and/or their member states, Switzerland, and the United Kingdom.
- “**European Data**” means Personal Data that is subject to the protection of European Data Protection Laws.
- “**European Data Protection Laws**” means data protection laws applicable in Europe, including: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (“GDPR”); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii); or (iii) UK GDPR as it applies as part of the United Kingdom’s domestic law via Section 3 of the European Union (Withdrawal) Act 2018 (“UK GDPR”); and (iv) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance (“Swiss DPA”); in each case, as may be amended, superseded or replaced.
- “**Instructions**” means the written, documented instructions issued by a Controller to a Processor, and directing the Processor to perform a specific or general action regarding Personal Data (including, but not limited to, depersonalizing, blocking, deletion, or making information available).

- **"Permitted Affiliates"** means any of your Affiliates that (i) are permitted to use the Subscription Services pursuant to the Master Terms but have not signed their own separate agreement with us and are not a "Customer" as defined under the Master Terms, (ii) qualify as a Controller of Personal Data Processed by us, and (iii) are subject to European Data Protection Laws .
- **"Personal Data"** means any information relating to an identified or identifiable individual where such information is contained within Customer Data and is protected similarly as personal data, personal information, or personally identifiable information under applicable Data Protection Laws.
- **"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed by us and/or our Sub-Processors in connection with the provision of the Subscription Services. "Personal Data Breach" will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.
- **"Processing"** means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, or erasure of Personal Data. The terms "Process", "Processes" and "Processed" will be construed accordingly.
- **"Processor"** means a natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of the Controller.
- **"Standard Contractual Clauses" or "SCC(s)"** means Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 04 June 2021, as currently set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.
- **"Sub-Processor"** means any Processor engaged by us or our Affiliates to assist in fulfilling our obligations with respect to the provision of the Subscription Services under the Master Terms. Sub-Processors may include third parties or our Affiliates but will exclude any ContractPod employee or consultant.
- **"Subscription Service(s)" or "Service(s)"** means the ContractPodAi platform, the ContractPodAi Cloud platform, and other Software-as-a-Service and/or software products provided by us, including, as applicable, implementation and consulting services provided by us to you as part of your purchase from us.
- **"You" or "Customer"** means the entity purchasing the Subscription Services from us, as identified on your Order Form.

II. Customer Responsibilities

- a) Compliance with Laws. You will be responsible for complying with all requirements that apply to you (as a Controller) in using the Subscription Services under applicable Data Protection Laws with respect to the Processing of Personal Data and the Instructions you issue to us.

This includes your acknowledgement and agreement that you will be solely responsible for:

- (i) the accuracy, integrity, and lawfulness of Personal Data you collected;
- (ii) complying with all applicable transparency and lawfulness requirements for the collection and use of the Personal Data, including obtaining any necessary consents and authorizations;
- (iii) ensuring you have the right to transfer, or provide access to, the Personal Data to us for Processing in accordance with the terms of the Master Terms (including this DPA);
- (iv) ensuring that your Instructions to us regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws; and
- (v) complying with all laws applicable to any emails or other content created, sent, or managed through the Subscription Services, including those relating to obtaining consents (where required).

You will inform us without undue delay if you are not able to comply with your responsibilities under this 'Compliance with Laws' section.

- b) Controller Instructions. The parties agree that the Master Terms (including this DPA), together with your use of the Subscription Services in accordance with the Master Terms, constitute your complete Instructions to us in relation to the Processing of Personal Data. You may, however, provide additional instructions during the subscription term so long as those instructions are consistent with the Master Terms, the nature of the Subscription Service, and the lawful use of the Subscription Service.

- c) **Security.** We take commercially reasonable precautions with respect to data security, as we discuss below. However, you are responsible for determining whether the data security provided in the Subscription Services adequately meets your obligations under applicable Data Protection Laws. As more fully set forth in the Master Terms, you are responsible for your secure use of the Subscription Services, including monitoring your employees and ensuring that secured systems, connections, and computers are used.

III. ContractPod Obligations

- a) **Compliance with Instructions.** We will comply with applicable Data Protection Laws that apply to us as a Processor when providing the Subscription Services. We will only Process Personal Data for the purposes described in this DPA or as otherwise agreed within the scope of your lawful Instructions, except when required by applicable law. We are not responsible for compliance with any Data Protection Laws applicable to you or your industry that are not generally applicable to us.
- b) **Conflict of Laws.** If we become aware that we cannot Process Personal Data in accordance with your Instructions due to a legal requirement under any applicable law, we will (i) promptly notify you of that legal requirement (to the extent permitted by the applicable law); and (ii) where necessary, cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as you issue new Instructions with which we are able to comply. If this provision is invoked, we will not be liable to you under the Master Terms for any failure to perform the applicable Subscription Services until such time as you issue new lawful Instructions regarding the Processing.
- c) **Security.** We will implement and maintain appropriate technical and organizational measures to protect Personal Data from Personal Data Breaches, as described under Annex B to this DPA ("Security Measures"). Notwithstanding any provision to the contrary, we may modify or update the Security Measures at our discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures.
- d) **Confidentiality.** We will ensure that any personnel whom we authorize to Process Personal Data on our behalf is subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to that Personal Data.
- e) **Personal Data Breaches.** We will notify you without undue delay after we become aware of any Personal Data Breach and will provide timely information relating to the Personal Data Breach as it becomes known or reasonably requested by you. At your request, we will promptly provide you with such reasonable assistance as necessary to enable you to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if you are required to do so under Data Protection Laws.
- f) **Deletion or Return of Personal Data.** In accordance with the procedures and timeframes set out in the Master Terms, we will delete or return all Customer Data, including Personal Data (including copies of such data) Processed pursuant to this DPA, on termination or expiration of your Subscription Services. This requirement will not apply if we are required by applicable law to retain some or all of the Customer Data, or to Customer Data we have archived on back-up systems, which we will securely isolate and protect from any further Processing and delete in accordance with our deletion practices. You may request the deletion of your account(s) after expiration or termination of your subscription, as well as a certificate of deletion, by submitting a request in our Data Subject Portal (when available), emailing privacy@contractpodai.com, or by contacting your ContractPod representative.

IV. Data Subject Requests.

- a) The Subscription Services provide you with several tools that you can use to retrieve, correct, delete, or restrict Personal Data, which you can use to assist in connection with your obligations under Data Protection Laws, including your obligations relating to responding to requests from Data Subjects to exercise their rights under applicable Data Protection Laws ("Data Subject Requests").
- b) To the extent that you are unable to independently address a Data Subject Request without our assistance, then upon your written request we will provide reasonable assistance to you to respond to any Data Subject Requests or requests from data protection authorities relating to the Processing of Personal Data under the Master Terms. You will reimburse us for the commercially reasonable costs arising from this assistance.
- c) If a Data Subject Request or other communication regarding the Processing of Personal Data under the Master Terms is made directly to us, we will promptly inform you and will advise the Data Subject to submit their request to you. You will be solely responsible for responding substantively to any such Data Subject Requests or communications involving Personal Data.

V. Sub-Processors.

You acknowledge and agree that (a) our Affiliates may be retained as Sub-Processors and (b) we and our Affiliates may engage Sub-Processors in connection with the provision of the Subscription Services. We have currently appointed, as Sub-Processors, the ContractPod Affiliates and third parties listed in Annex C to this DPA. We will notify you if we add or remove Sub-Processors to Annex C prior to any such changes.

Where we engage Sub-Processors, we will impose data protection terms on the Sub-Processors that provide at least the same level of protection for Personal Data as those in this DPA (including, where appropriate, the Standard Contractual Clauses), to the extent applicable to the nature of the services provided by such Sub-Processors. We will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause us to breach any of its obligations under this DPA.

VI. Data Transfers.

You acknowledge and agree that we may access and Process Personal Data on a global basis as necessary to provide the Services in accordance with the Master Terms, and that Personal Data may be transferred to the United States and to other jurisdictions where ContractPod Affiliates and Sub-Processors have operations to meet and comply with our support obligations. Wherever Personal Data is transferred outside of its country of origin, each party will ensure such transfers are made in compliance with the requirements of Data Protection Laws.

VII. Additional Provisions for European Data.

- a) Scope of Section VII. This "Additional Provisions for European Data" section will apply only with respect to European Data.
- b) Transfer Mechanisms for Data Transfers.
 - 1) ContractPod will not transfer European Data to any country or recipient not recognized as providing an adequate level of protection for Personal Data (within the meaning of applicable European Data Protection Laws), unless it first takes all such measures as are necessary to ensure the transfer follows applicable European Data Protection Laws. Such measures may include (without limitation) transferring such data to a recipient that is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, to a recipient that has achieved binding corporate rules authorization in accordance with European Data Protection Laws, or to a recipient that has executed appropriate standard contractual clauses in each case as adopted or approved in accordance with applicable European Data Protection Laws.
 - 2) You acknowledge that in connection with the performance of the Subscription Services, ContractPod USA Inc. is a recipient of European Data in the United States. ContractPod Technologies Limited and ContractPod USA agree to abide by and process European Data in compliance with the Standard Contractual Clauses.
- c) Operative Provisions and Additional Terms. The parties agree that, for the purposes of the Standard Contractual Clauses:
 - 1) *Roles of the Parties.* When Processing European Data in accordance with your Instructions, the parties acknowledge and agree that you are the Controller of European Data and we are the Processor. The Parties will comply with the SCC Module Two: Transfer Controller-to-Processor, subject to this § VII.
 - 2) *Relevant Provisions.* The relevant provisions contained in the Standard Contractual Clauses, Module Two: Transfer Controller-to-Processor are incorporated by reference and are an integral part of this DPA.
 - 3) *Annexes.* The Annexes of the Standard Contractual Clauses will be populated with the relevant information set out in Annex A, Annex B, and Annex C of this DPA.
 - 4) *Instructions.* This DPA and the Master Terms are your complete and final documented instructions at the time of signature of the Order Form to us for the Processing of Personal Data. Any additional or alternate instructions must be consistent with the terms of this DPA and the Master Terms. For the purposes of SCC Clause 8.1(a), the instructions by you to Process Personal Data are set out in this DPA and include onward transfers to a third party located outside Europe for the purpose of the performance of the Subscription Services. If we believe that your Instruction infringes European Data Protection Laws (where applicable), we will inform you without delay.
 - 5) *Certification of Deletion.* The parties agree that the certification of deletion of Personal Data that is described in SCC Clauses 8.5 and 16(d) will be provided by us to you only upon your written request.
 - 6) *Security of Processing.* For the purposes of SCC Clause 8.6(a), as set forth in § II(c) of this DPA, Customer is solely responsible for making an independent determination as to whether our technical and organizational measures meet Customer's requirements and agrees that, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the Processing of its Personal Data as well as the risks to individuals, the security measures and policies we have implemented and maintained provide a level of security appropriate to the risk with respect to its Personal Data. For the purposes of clause 8.6(c), personal data breaches will be handled in accordance with § III(e) of this DPA.
 - 7) *Audits of the SCCs.* We will make all information reasonably necessary to demonstrate compliance with this DPA available to you and allow for and contribute to audits, including inspections by you or your auditor to assess

compliance with this DPA and Clause 8.9 of the SCCs. You agree that you will exercise your audit rights under this DPA by instructing us to comply with the audit measures described in this § VII(c)(7). You acknowledge that the Subscription Services are hosted by our data center partners who maintain independently validated security programs (including SOC 2 and ISO 27001) and that our systems are regularly tested by independent third-party penetration testing firms. Upon your written request, we will supply (on a strictly confidential basis) a summary copy of our penetration testing report(s) to you so that you can verify our compliance with this DPA. Further, at your written request, we will provide written responses (again, on a strictly confidential basis) to reasonable requests for information made by you necessary to confirm our compliance with this DPA, but you will not exercise this right more than once per calendar year (unless you have reasonable grounds to suspect our non-compliance with this DPA).

- 8) *General Authorization for Use of Sub-Processors; Notification & Objection Process.*
 - i. Option 2 under SCC Clause 9 applies. For the purposes of SCC Clause 9(a), we have your general authorization to engage Sub-Processors in accordance with § V of this DPA. You acknowledge and expressly agree that we may engage new Sub-processors as described in § V of this DPA. We will inform you of any changes to Sub-Processors following the procedure provided for in § V of this DPA.
 - ii. We will give you the opportunity to object to the engagement of new Sub-Processors on reasonable grounds related to the protection of Personal Data. If you do object, you must do so within 30 days of our notifying you in accordance with § V, "Sub-Processors". If you do notify us of such an objection, the parties will discuss your concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, we will, at our sole discretion, either not appoint the new Sub-Processor, or permit you to suspend or terminate the affected Subscription Service in accordance with the termination provisions of the Master Terms without liability to either party (but without prejudice to any fees incurred by you prior to suspension or termination). *The parties agree that by complying with this § VII(8), we fulfill our obligations under Clause 9 of the Standard Contractual Clauses.*
- 9) *Sub-Processor Agreements.* For the purposes of Clause 9(c) of the Standard Contractual Clauses, you acknowledge that we may be restricted from disclosing Sub-Processor agreements but that we will use reasonable efforts to require any Sub-Processor we appoint (i) to permit us to disclose the Sub-Processor agreement to you and (ii) to provide, on a strictly confidential basis, the information that we reasonably can.
- 10) *Complaints - Redress.* For the purposes of SCC Clause 11, and subject to § IV of this DPA, we will inform data subjects of your contact point authorized to handle complaints. We will inform you if we receive a complaint by, or a dispute from, a Data Subject with respect to Personal Data and will promptly communicate the complaint or dispute to you. We will not otherwise have any obligation to handle the request (unless otherwise agreed with you). The option under clause 11 does not apply.
- 11) *Liability.* Our liability under SCC Clause 12(b) is limited to any damage caused by our Processing where we have not complied with our obligations under the applicable Data Protection Laws as specifically directed to Processors, or where we have acted outside of, or contrary to, your lawful instructions, as specified in Article 82 GDPR. This limitation is in addition to § IX(c) of this DPA.
- 12) *Data Protection Impact Assessments and Consultation with Supervisory Authorities.* To the extent that the required information is reasonably available to us, and you do not otherwise have access to the required information, we will provide reasonable assistance to you with any data protection impact assessments, and prior consultations with supervisory authorities or other competent data privacy authorities to the extent required by European Data Protection Laws.
- 13) *Notification of Government Access Requests.* For the purposes of clause 15(1)(a), we will notify you and not the Data Subject(s) in case of government access requests. You will be solely responsible for promptly notifying the Data Subject as necessary.
- 14) *Inability to Comply.* If we cannot comply with our obligations under the Standard Contractual Clauses or we are in breach of any warranties under the SCCs, and as a result you intend to suspend the transfer of European Data to us or terminate the SCCs, you agree to provide us with reasonable notice to allow us to cure such alleged non-compliance and reasonably cooperate with us to identify what additional safeguards (if any) may be implemented to remedy the alleged non-compliance. If we will not or cannot cure the non-compliance, you will have the right to terminate or suspend the affected portion of the Subscription Services in accordance with the Master Terms without further liability to either party (but you will remain responsible for any fees incurred prior to suspension or termination).
- 15) *Governing Law.* The governing law for the purposes of SCC Clause 17 will be the law that is designated in the Governing Law section of this DPA. If the DPA is not governed by an EU Member State law, the Standard Contractual Clauses will be governed by either (i) the laws of the Netherlands; or (ii) where the DPA is governed by the laws of the United Kingdom, the laws of the United Kingdom.

16) *Choice of Forum and Jurisdiction*. The courts under clause 18 will be those designated in § IX(d) of the DPA, with the modification that the parties agree that either the courts of the Netherlands (as specified in § IX(d)(2)(i) of the DPA) or the United Kingdom will have jurisdiction. For Data Subjects habitually resident in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect of disputes.

- d) Data Exports from the United Kingdom and Switzerland under the Standard Contractual Clauses. If transfers of Personal Data from the United Kingdom are subject exclusively to the UK GDPR or transfers of Personal Data from Switzerland are subject exclusively to the Swiss DPA, general and specific references and obligations in the Standard Contractual Clauses to GDPR or EU or Member State Law will have the same meaning as the equivalent reference in the UK GDPR or Swiss DPA (as applicable).
- e) Regarding ContractPod USA. If the ContractPod contracting entity in your Order Form is *not* ContractPod USA, that contracting entity (not ContractPod USA) will remain fully and solely responsible and liable to you for the performance of the Standard Contractual Clauses by ContractPod USA and you will direct any instructions, claims, or questions to that contracting entity.
- f) Conflicts with the SCCs. If there is any conflict between the provisions of this DPA and the Standard Contractual Clauses, the SCCs will prevail (but only to the extent of the conflict).

VIII. Additional Provisions for California Personal Information.

- a) Scope of this Section VIII. The “Additional Provisions for California Personal Information” section of this DPA will apply only with respect to California Personal Information.
- b) Roles of the Parties. When processing California Personal Information in accordance with your Instructions, the parties acknowledge and agree that you are a Business and we are a Service Provider for the purposes of the CCPA.
- c) Responsibilities. The parties agree that we will Process California Personal Information as a Service Provider strictly for the purpose of performing the Subscription Services under the Master Terms (the “Business Purpose”) or as otherwise permitted by the CCPA and for no other commercial purposes.

IX. General Provisions.

- a) Amendments. Notwithstanding anything else to the contrary in the Master Terms and without prejudice to the “Compliance with Instructions” or “Security” sections of this DPA, we reserve the right to make any updates and changes to this DPA and the terms that apply in the relevant modification section (regardless of name) of the Master Terms will apply. If these changes are material and alter a party’s obligations under this DPA, we will (if legally permissible) provide you with at least 10 days’ notice of such changes (typically by posting a message on our website and contacting you by email), so that you may respond.
- b) Severability. If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA will not be affected.
- c) Limitation of Liability. Each party and each of their Affiliates’ liability, taken in aggregate, arising out of or related to this DPA (and any other DPAs between the parties) and the Standard Contractual Clauses (where applicable), whether in contract, tort, or under any other theory of liability, will be subject to the limitations and exclusions of liability set out in the “Limitation of Liability” section of the Master Terms and any reference in such section to the liability of a party means aggregate liability of that party and all of its Affiliates under the Master Terms (including all DPAs). In no event will either party’s liability be limited with respect to any individual’s data protection rights where such limitation is prohibited by applicable Data Protection Laws.
- d) Governing Law. Unless otherwise required by the applicable Data Protection Laws, this DPA will be governed by and construed in accordance with:
 - 1) If your Master Terms are with ContractPod Technologies Inc., the governing law is the law of the State of New York and applicable law of the United States, with exclusive jurisdiction in the State of New York, and exclusive forum of either the United States District Court for the Southern District of New York or the New York State Supreme Court, Commercial Division, Manhattan (as applicable); or
 - 2) If your Master Terms are with ContractPod Technologies Limited, the governing law is the law of England & Wales and applicable United Kingdom law, with exclusive jurisdiction in London, England.
 - i. However, at a party’s election, if your Master Terms are with ContractPod Technologies Limited, the parties may instead resolve their dispute in the Amsterdam District Court following proceedings in English before the Chamber for International Commercial Matters (“Netherlands Commercial Court” or “NCC District Court”). An action for interim measures, including protective measures, available under Dutch law may be brought in the NCC’s Court in Summary Proceedings (CSP) in proceedings in English. Any appeals against NCC or CSP judgments will be submitted to the Amsterdam Court of Appeal’s Chamber for International Commercial Matters (“Netherlands Commercial Court of Appeal” or “NCCA”). The NCC Rules of Procedure will apply.

X. Parties to this DPA.

- a) **Permitted Affiliates.** By signing your Order Form (and thereby accepting the Master Terms), you enter into this DPA (and as applicable the SCCs) on behalf of yourself and in the name and on behalf of your Permitted Affiliates. For the purposes of this DPA only, and except where indicated otherwise, the terms “Customer”, “you” and “your” will include you and such Permitted Affiliates.
- b) **Authorization.** The legal entities agreeing to this DPA represents that they are authorized to agree to and enter into this DPA for and on behalf of themselves and, as applicable, each of their Affiliates and/or Permitted Affiliates.
- c) **Remedies.** The parties agree that (i) solely the Customer entity that is the contracting party to the Master Terms will exercise any right or seek any remedy any Permitted Affiliate may have under this DPA on behalf of its Affiliates, and (ii) the Customer entity that is the contracting party to the Master Terms will exercise any such rights under this DPA not separately for each Permitted Affiliate individually but in a combined manner for itself and all of its Permitted Affiliates together. The Customer entity that is the contracting entity is responsible for coordinating all Instructions, authorizations, and communications with us under the DPA and will be entitled to make and receive any communication related to this DPA on behalf of its Permitted Affiliates.
- d) **Other rights.** You will, when reviewing our compliance with this DPA pursuant to the “Demonstration of Compliance” section, take all reasonable measures to limit any impact on us and our Affiliates by combining several audit requests carried out on behalf of the Customer entity that is the contracting party to the Master Terms and all of its Permitted Affiliates in one single audit.

ANNEX A Details of Processing

1) List of Parties.

a) Data Exporter(s).

- i) *Name:* Customer and its Permitted Affiliates
- ii) *Address:* The Customer's Address, as set out in the Order Form.
- iii) *Contact Person's Name, Position, and Contact Details:* The Customer's contact details, as set out in the Order Form or as updated from time-to-time with ContractPod.
- iv) *Activities relevant to the data transferred under these Clauses:* Processing of Personal Data (if any) in connection with Customer and its Permitted Affiliates usage of the ContractPod Subscription Services under the Master Terms.
- v) *Role:* If the EU Controller-to-Processor Clauses apply, then Customer and/or its Permitted Affiliates are a Controller.

b) Data Importer.

- i) *Name:* ContractPod Technologies Inc.
- ii) *Address:* 135 East 57th Street, 11th Floor, New York City, New York, 10022 USA
- iii) *Contact Person's Name, Position, and Contact Details:* Bill Fitzgerald, Director of Information Security, privacy@contractpodai.com
- iv) *Activities relevant to the data transferred under these Clauses:* Processing of Personal Data (if any) in connection with Customer and its Permitted Affiliates usage of the ContractPod Subscription Services under the Master Terms.
- v) *Role:* Processor.

2) Categories Of Data Subjects Whose Personal Data Is Transferred.

- a) Customer may submit Personal Data to the Subscription Services, 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:
 - i) Prospects, customers, business partners and vendors of Customer (who are natural persons),
 - ii) Employees or contact persons of Customer's prospects, customers, business partners and vendors,
 - iii) Employees, agents, advisors, freelancers of Customer (who are natural persons), or
 - iv) Customer's Users authorized by Customer to use the Services.

3) Categories Of Personal Data Transferred.

- a) Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

i) First and last name	vi) ID data
ii) Title	vii) Professional life data
iii) Position	viii) Personal life data
iv) Employer	ix) Localization data
v) Contact information (company, email, phone, physical business address)	

- 4) **Sensitive Data Transferred and Applied Restrictions or Safeguards.** The parties do not anticipate the transfer of special categories of data.
- 5) **Frequency of the Transfer.** As and when authorized basis depending on the use of the Subscription Services by Customer.
- 6) **Nature of the Processing.** The performance of the Subscription Services pursuant to the applicable Order Form and the Master Terms.
- 7) **Purpose of Processing, The Data Transfer, and Further Processing.** We will Process Personal Data as necessary to perform the Subscription Services pursuant to the Order Form, the Master Terms, and as further instructed by the Customer in its use of the Subscription Services.

- 8) **Duration of Processing.** Subject to the “Deletion or Return of Personal Data” section of this DPA, we will Process Personal Data for the duration of the Master Terms, unless otherwise agreed in writing.
- 9) **Sub-Processor Transfers.** The subject matter (category of data) and the nature of the data for Sub-Processors are the same as those listed above in Description of Transfer, subsection B. The Sub-processor will Process Personal Data for the duration of the Master Terms, unless otherwise agreed in writing.
- 10) **Competent Supervisory Authority.** For the purposes of the Standard Contractual Clauses, the supervisory authority that will act as competent supervisory authority is as follows:
 - a) Where Customer is established in an EU Member State, the supervisory authority responsible for ensuring Customer's compliance with the GDPR;
 - b) Where Customer is not established in an EU Member State but falls within the extra-territorial scope of the GDPR and has appointed a representative, the supervisory authority of the EU Member State in which Customer's representative is established;
 - c) Where Customer is not established in an EU Member State but falls within the extra-territorial scope of the GDPR without having to appoint a representative, the supervisory authority of the EU Member State in which the Data Subjects are predominantly located.
 - d) With relation to Personal Data that is subject to the UK GDPR or Swiss DPA, the competent supervisory authority is the UK Information Commissioner or the Swiss Federal Data Protection and Information Commissioner (as applicable).

ANNEX B Security Measures

This Annex B forms part of the DPA.

We currently observe the Security Measures described in this Annex B. These safeguards are without prejudice to us taking *more protective measures* but are the minimum security measures we have implemented.

1. Strong encryption of Personal Data in transit and at rest, as applicable, in accordance with industry practices, and which is robust against cryptanalysis, is not susceptible to interference or unauthorized access, and for which key access is limited to specific authorized individuals with a need to access Personal Information in order to engage in Processing or, wherever practicable, such key access is limited solely to the exporter;
2. Wherever practicable with respect to Processing, pseudonymization sufficient to cause Personal Data to no longer be attributable to a specific individual, provided safeguards are in place to prevent reidentification and the algorithmic process or key to re-establish identity is held only by the data exporter;
3. Access restrictions and procedures, including unique user identification, to limit Processing to authorized ContractPodAi workforce and devices authorized explicitly by ContractPodAi through proper separation of duties, role-based access, on a need-to-know and least privilege basis;
4. Multi-factor authentication and use of a virtual private network for any remote access to ContractPodAi systems or Personal Information;
5. Physical security procedures, including the use of monitoring 24 hours /7 days a week, access controls and logs of access, and measures sufficient to prevent physical intrusions to any ContractPodAi facility where Personal Data is Processed;
6. Secure disposal of equipment and physical and electronic media that contain Personal Data in accordance with generally accepted sanitation processes (such as NIST SP 800-88);
7. Ongoing vulnerability identification, management and remediation of systems including applications, databases, and operating systems used by ContractPodAi to Process Personal Data;
8. Logging and monitoring to include security events, all critical assets that Process Personal Data, and system components that perform security functions for ContractPodAi's network (e.g., firewalls, IDS/IPS, authentication servers) intended to identify actual or attempted access by unauthorized individuals and anomalous behavior by authenticated users;
9. Monitoring, detecting, and restricting the flows of Personal Data on a multi-layered basis, including but not limited to the use of network segmentation, secure configuration of firewalls, intrusion detection and/or prevention systems, denial of service protections;
10. Remote work procedures that require "clean desk" standards in place and a remote work management program that limits use to only devices authorized pursuant to ContractPodAi's security program;
11. Data protection program elements, such as technical measures or documented procedures, to address data minimization and limited retention, data quality, and implementation of data subject rights, appropriate to the nature of the Processing and Services;
12. Appropriate IT governance processes that address risk management, system configuration, and process assurance, including regular and periodic testing and evaluation of the sufficiency of ContractPodAi's data protection program and technical controls;
13. Business continuity and disaster recovery plans intended to ensure integrity, resiliency, and availability of Vendor systems and Personal Information, as well as timely restoration of access to Personal Data; and
14. ContractPodAi will, at the request of data exporter, promptly provide a copy of its most recent Vendor SOC2 Type II report, other industry certifications, and/or any successor standards for information security management that ContractPodAi has obtained.

ANNEX C List of Sub-Processors

Sub-Processor	Purpose	Location
IBM Watson	Utilizing artificial intelligence to abstract contract metadata information against a record.	EU
Zuva Inc.	Document Intelligence	USA Japan
Microsoft Azure Services	Data Hosting, Translation	EU (for UK and EU-based Customers) USA (for USA-based Customers) Australia (for APAC-based Customers)
ABBY OCR SDK	Converting pdf and scanned document in a format acceptable to IBM Watson for AI processing	EU
DocuSign	Electronic signature	EU (for UK and EU-based Customers) USA (for USA-based Customers)
ContractPod Solutions Pvt. Ltd. (a wholly owned subsidiary of ContractPod Technologies Limited)	Services & Support	Republic of India
ContractPod Technologies Inc. (a wholly owned subsidiary of ContractPod Technologies Limited)	Services & Support	United States of America
ContractPod Technologies Ltd.	Services & Support	United Kingdom Canada
ContractPod Technologies (Asia Pacific) Pty. Ltd.	Services & Support	Australia