

## Annex B: Bonterms Data Processing Addendum

### DPA Setup Page

The DPA includes the contents of this DPA Setup Page, including the Key Terms, Schedules and any Additional Terms set forth below. Capitalized terms not defined in this DPA Setup Page have the meanings given in the Data Protection Addendum.

#### Key Terms

<b>Agreement</b>	This DPA is an Attachment to the Order Form and Agreement between «Client_Name» (“Customer”) and «Legal_Party_Name» (“Provider”), with ContractPodAi Request ID: #«Request_ID».
------------------	---

<b>DPA Effective Date</b>	Effective the date of the referenced Order Form and Agreement between Customer and Provider.
---------------------------	--

	Sub-Processor	Purpose	Location	Products Used In
<b>Subprocessor List†</b>	<b>ABBY OCR SDK</b>	Converting pdf and scanned document in a format acceptable to IBM Watson for AI processing	EU	CLM
	<b>Anthropic PBC</b>	Leah Functionality (no Customer Data is stored or retained by Anthropic)	USA Japan EU / UK	Leah
	<b>Cohere, Inc.</b>	Leah Functionality (no Customer Data is stored or retained by Cohere)	Canada USA EU / UK Japan	Leah
	<b>ContractPod Solutions Pvt. Ltd.</b>	Services & Support	Republic of India	All (When Necessary)
	<b>ContractPod Technologies (Asia Pacific) Pty. Ltd.</b>	Services & Support	Australia	All (When Necessary)
	<b>ContractPod Technologies Inc.</b>	Services & Support	United States of America	All (When Necessary)
	<b>ContractPod Technologies Ltd.</b>	Services & Support	United Kingdom Canada	All (When Necessary)
	<b>DocuSign or Adobe Inc.</b>	Electronic signature	EU USA	CLM
	<b>Google AI/ML; Google Cloud</b>	Leah Functionality (no Customer Data is stored or retained by Google); Data hosting for Google Cloud Customers	USA Japan EU / CH / UK	Leah
	<b>Jitterbit</b>	API connectivity for non-standard integrations.	EU US	CLM

† Not all subprocessors will be applicable to all ContractPodAi customers. For example, depending on your eSignature solution, either DocuSign or AdobeSign will be used, to the exclusion of the other.

	<b>Microsoft Azure Services</b>	Data Hosting, Translation, Microsoft Office Services (if using WOPI services)	EU USA Australia	CLM Leah
	<b>OpenAI LLC</b>	Leah Functionality (no Customer Data is stored or retained by OpenAI)	USA Japan EU / CH	Leah
	<b>QlikTech International AB</b>	Reporting and Graphing for DeepSights	Ireland, Frankfurt, London (UK/EU/CH) USA Australia, Singapore (APAC)	CLM
	<b>Sendgrid</b>	Email Send Service	USA	CLM
	<b>ZOHO Corporation Pvt. Ltd.</b>	Document collaboration (if using ZOHO services)	EU	CLM
	<b>Zuva Inc.</b>	Document Intelligence	USA Japan EU	CLM

Schedules <i>(attach)</i>	
The following Schedules are incorporated into this DPA:	
<b>Schedule 1: Subject Matter and Details of Processing</b>	
<b>Schedule 2: Technical and Organizational Measures</b>	
<b>Schedule 3: Cross-Border Transfer Mechanisms</b>	
<b>Schedule 4: Region-Specific Terms</b>	

Additional Terms	
The following additions to or modifications of the Bonterms Data Protection Addendum are agreed by the parties and control in the event of any conflicts:	

## Bonterms Data Protection Addendum (DPA) (Version 1.0)

This Data Protection Addendum (“**DPA**”) is an Attachment to the **Agreement**. Customer and Provider enter into this DPA by executing a DPA Setup Page. Capitalized terms not defined in this DPA are defined in the Agreement or DPA Setup Page.

### 1. Definitions.

- 1.1. “**Agreement**” means the Agreement between Customer and Provider incorporating the Bonterms Cloud Terms which is specified on the DPA Setup Page.
- 1.2. “**Audit**” and “**Audit Parameters**” are defined in Section 9.3 below.
- 1.3. “**Audit Report**” is defined in Section 9.2 below.
- 1.4. “**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 Processing of Personal Data.
- 1.5. “**Customer Instructions**” is defined in Section 3.1 below.
- 1.6. “**Customer Personal Data**” means Personal Data in Customer Data (as defined in the Agreement).
- 1.7. “**Data Protection Laws**” means all laws and regulations applicable to the Processing of Customer Personal Data under the Agreement, including, as applicable: (i) the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and any binding regulations promulgated thereunder (“**CCPA**”), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) (“**EU GDPR**” or “**GDPR**”), (iii) the Swiss Federal Act on Data Protection (“**FADP**”), (iv) the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the “**UK GDPR**”) and (v) the UK Data Protection Act 2018; in each case, as updated, amended or replaced from time to time.
- 1.8. “**Data Subject**” means the identified or identifiable natural person to whom Customer Personal Data relates.
- 1.9. “**DPA Effective Date**” is specified on the DPA Setup Page.
- 1.10. “**DPA Setup Page**” means a separate document executed by Customer and Provider which causes this DPA to become an Attachment to their Agreement.
- 1.11. “**EEA**” means European Economic Area.
- 1.12. “**Key Terms**” means Agreement, DPA Effective Date and Subprocessor List as specified by the parties on the DPA Setup Page.
- 1.13. “**Personal Data**” means information about an identified or identifiable natural person or which otherwise constitutes “personal data”, “personal information”, “personally identifiable information” or similar terms as defined in Data Protection Laws.
- 1.14. “**Processing**” and inflections thereof refer to any operation or set of operations that is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- 1.15. “**Processor**” means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.
- 1.16. “**Restricted Transfer**” means: (i) where EU GDPR applies, a transfer of Customer Personal Data from the EEA to a country outside the EEA that is not subject to an adequacy determination, (ii) where UK GDPR applies, a transfer of Customer Personal Data from the United Kingdom to any other country that is not subject to an adequacy determination or (iii) where FADP applies, a transfer of Customer Personal Data from Switzerland to any other country that is not subject to an adequacy determination.
- 1.17. “**Schedules**” means one or more schedules incorporated by the parties in their DPA Setup Page. The default Schedules for this DPA are:

Schedule 1	Subject Matter and Details of Processing
Schedule 2	Technical and Organizational Measures
Schedule 3	Cross-Border Transfer Mechanisms
Schedule 4	Region-Specific Terms

- 1.18. “**Security Incident**” means any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data being Processed by Provider.

- 1.19. “**Specified Notice Period**” is 48 hours.
- 1.20. “**Subprocessor**” means any third party authorized by Provider to Process any Customer Personal Data.
- 1.21. “**Subprocessor List**” means the list of Provider’s Subprocessors as identified or linked to on the DPA Setup Page.

## 2. Scope and Duration.

- 2.1. Roles of the Parties. This DPA applies to Provider as a Processor of Customer Personal Data and to Customer as a Controller or Processor of Customer Personal Data.
- 2.2. Scope of DPA. This DPA applies to Provider’s Processing of Customer Personal Data under the Agreement to the extent such Processing is subject to Data Protection Laws. This DPA is governed by the governing law of the Agreement unless otherwise required by Data Protection Laws.
- 2.3. Duration of DPA. This DPA commences on the **DPA Effective Date** and terminates upon expiration or termination of the Agreement (or, if later, the date on which Provider has ceased all Processing of Customer Personal Data).
- 2.4. Order of Precedence. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) any Standard Contractual Clauses or other measures to which the parties have agreed in Schedule 3 (Cross-Border Transfer Mechanisms) or Schedule 4 (Region-Specific Terms), (2) this DPA and (3) the Agreement. To the fullest extent permitted by Data Protection Laws, any claims brought in connection with this DPA (including its Schedules) will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations, set forth in the Agreement.

## 3. Processing of Personal Data.

### 3.1. Customer Instructions.

- (a) Provider will Process Customer Personal Data as a Processor only: (i) in accordance with Customer Instructions or (ii) to comply with Provider’s obligations under applicable laws, subject to any notice requirements under Data Protection Laws.
- (b) “**Customer Instructions**” means: (i) Processing to provide the Cloud Service and perform Provider’s obligations in the Agreement (including this DPA) and (ii) other reasonable documented instructions of Customer consistent with the terms of the Agreement.
- (c) Details regarding the Processing of Customer Personal Data by Provider are set forth in Schedule 1 (Subject Matter and Details of Processing).
- (d) Provider will notify Customer if it receives an instruction that Provider reasonably determines infringes Data Protection Laws (but Provider has no obligation to actively monitor Customer’s compliance with Data Protection Laws).

### 3.2. Confidentiality.

- (a) Provider will protect Customer Personal Data in accordance with its confidentiality obligations as set forth in the Agreement.
- (b) Provider will ensure personnel who Process Customer Personal Data either enter into written confidentiality agreements or are subject to statutory obligations of confidentiality.

### 3.3. Compliance with Laws.

- (a) Provider and Customer will each comply with Data Protection Laws in their respective Processing of Customer Personal Data.
- (b) Customer will comply with Data Protection Laws in its issuing of Customer Instructions to Provider. Customer will ensure that it has established all necessary lawful bases under Data Protection Laws to enable Provider to lawfully Process Customer Personal Data for the purposes contemplated by the Agreement (including this DPA), including, as applicable, by obtaining all necessary consents from, and giving all necessary notices to, Data Subjects.

- 3.4. Changes to Laws. 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 Data Protection Laws from time to time.

## 4. Subprocessors.

### 4.1. Use of Subprocessors.

- (a) Customer generally authorizes Provider to engage Subprocessors to Process Customer Personal Data. Customer further agrees that Provider may engage its Affiliates as Subprocessors.
- (b) Provider will: (i) enter into a written agreement with each Subprocessor imposing data Processing and protection obligations substantially the same as those set out in this DPA and (ii) remain liable for compliance with the obligations of this DPA and for any acts or omissions of a Subprocessor that cause Provider to breach any of its obligations under this DPA.

- 4.2. Subprocessor List. Provider will maintain an up-to-date list of its Subprocessors, including their functions and locations, as

specified in the **Subprocessor List**.

4.3. **Notice of New Subprocessors.** Provider may update the **Subprocessor List** from time to time. At least 30 days before any new Subprocessor Processes any Customer Personal Data, Provider will add such Subprocessor to the **Subprocessor List** and notify Customer through email or other means specified on the DPA Setup Page.

4.4. **Objection to New Subprocessors.**

- (a) If, within 30 days after notice of a new Subprocessor, Customer notifies Provider in writing that Customer objects to Provider's appointment of such new Subprocessor based on reasonable data protection concerns, the parties will discuss such concerns in good faith.
- (b) If the parties are unable to reach a mutually agreeable resolution to Customer's objection to a new Subprocessor, Customer, as its sole and exclusive remedy, may terminate the Order for the affected Cloud Service for convenience and Provider will refund any prepaid, unused fees for the terminated portion of the Subscription Term.

## 5. Security.

5.1. **Security Measures.** Provider will implement and maintain reasonable and appropriate technical and organizational measures, procedures and practices, as appropriate to the nature of the Customer Personal Data, that are designed to protect the security, confidentiality, integrity and availability of Customer Personal Data and protect against Security Incidents, in accordance with Provider's Security Measures referenced in the Agreement and as further described in **Schedule 2** (Technical and Organizational Measures). Provider will regularly monitor its compliance with its Security Measures and **Schedule 2** (Technical and Organizational Measures).

5.2. **Incident Notice and Response.**

- (a) Provider will implement and follow procedures to detect and respond to Security Incidents.
- (b) Provider will: (i) notify Customer without undue delay and, in any event, not later than the Specified Notice Period, after becoming aware of a Security Incident affecting Customer and (ii) make reasonable efforts to identify the cause of the Security Incident, mitigate the effects and remediate the cause to the extent within Provider's reasonable control.
- (c) Upon Customer's request and taking into account the nature of the applicable Processing, Provider will assist Customer by providing, when available, information reasonably necessary for Customer to meet its Security Incident notification obligations under Data Protection Laws.
- (d) Customer acknowledges that Provider's notification of a Security Incident is not an acknowledgement by Provider of its fault or liability.
- (e) Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful login attempts, pings, port scans, denial of service attacks or other network attacks on firewalls or networked systems.

5.3. **Customer Responsibilities.**

- (a) Customer is responsible for reviewing the information made available by Provider relating to data security and making an independent determination as to whether the Cloud Service meets Customer's requirements and legal obligations under Data Protection Laws.
- (b) Customer is solely responsible for complying with Security Incident notification laws applicable to Customer and fulfilling any obligations to give notices to government authorities, affected individuals or others relating to any Security Incidents.

6. **Data Protection Impact Assessment.** Upon Customer's request and taking into account the nature of the applicable Processing, to the extent such information is available to Provider, Provider will assist Customer in fulfilling Customer's obligations under Data Protection Laws to carry out a data protection impact or similar risk assessment related to Customer's use of the Cloud Service, including, if required by Data Protection Laws, by assisting Customer in consultations with relevant government authorities.

## 7. Data Subject Requests.

7.1. **Assisting Customer.** Upon Customer's request and taking into account the nature of the applicable Processing, Provider will assist Customer by appropriate technical and organizational measures, insofar as possible, in complying with Customer's obligations under Data Protection Laws to respond to requests from individuals to exercise their rights under Data Protection Laws, provided that Customer cannot reasonably fulfill such requests independently (including through use of the Cloud Service).

7.2. **Data Subject Requests.** If Provider receives a request from a Data Subject in relation to the Data Subject's Customer Personal Data, Provider will notify Customer and advise the Data Subject to submit the request to Customer (but not otherwise communicate with the Data Subject regarding the request except as may be required by Data Protection Laws), and Customer will be responsible for responding to any such request.

## 8. Data Return or Deletion.

- 8.1. During Subscription Term. During the Subscription Term, Customer may, through the features of the Cloud Service or such other means specified on the DPA Setup Page, access, return to itself or delete Customer Personal Data.
- 8.2. Post Termination.
  - (a) Following termination or expiration of the Agreement, Provider will, in accordance with its obligations under the Agreement, delete all Customer Personal Data from Provider’s systems.
  - (b) Deletion will be in accordance with industry-standard secure deletion practices. Provider will issue a certificate of deletion upon Customer’s request.
  - (c) Notwithstanding the foregoing, Provider may retain Customer Personal Data: (i) as required by Data Protection Laws or (ii) in accordance with its standard backup or record retention policies, provided that, in either case, Provider will (x) maintain the confidentiality of, and otherwise comply with the applicable provisions of this DPA with respect to, retained Customer Personal Data and (y) not further Process retained Customer Personal Data except for such purpose(s) and duration specified in such applicable Data Protection Laws.

**9. Audits.**

- 9.1. Provider Records Generally. Provider will keep records of its Processing in compliance with Data Protection Laws and, upon Customer’s request, make available to Customer any records reasonably necessary to demonstrate compliance with Provider’s obligations under this DPA and Data Protection Laws.
- 9.2. Third-Party Compliance Program.
  - (a) Provider will describe its third-party audit and certification programs (if any) and make summary copies of its audit reports (each, an “**Audit Report**”) available to Customer upon Customer’s written request at reasonable intervals (subject to confidentiality obligations).
  - (b) Customer may share a copy of Audit Reports with relevant government authorities as required upon their request.
  - (c) Customer agrees that any audit rights granted by Data Protection Laws will be satisfied by Audit Reports and the procedures of Section 9.3 (Customer Audit) below.
- 9.3. Customer Audit.
  - (a) Subject to the terms of this Section 9.3, Customer has the right, at Customer’s expense, to conduct an audit of reasonable scope and duration pursuant to a mutually agreed-upon audit plan with Provider that is consistent with the Audit Parameters (an “**Audit**”).
  - (b) Customer may exercise its Audit right: (i) to the extent Provider’s provision of an Audit Report does not provide sufficient information for Customer to verify Provider’s compliance with this DPA or the parties’ compliance with Data Protection Laws, (ii) as necessary for Customer to respond to a government authority audit or (iii) in connection with a Security Incident.
  - (c) Each Audit must conform to the following parameters (“**Audit Parameters**”): (i) be conducted by an independent third party that will enter into a confidentiality agreement with Provider, (ii) be limited in scope to matters reasonably required for Customer to assess Provider’s compliance with this DPA and the parties’ compliance with Data Protection Laws, (iii) occur at a mutually agreed date and time and only during Provider’s regular business hours, (iv) occur no more than once annually (unless required under Data Protection Laws or in connection with a Security Incident), (v) cover only facilities controlled by Provider, (vi) restrict findings to Customer Personal Data only and (vii) treat any results as confidential information to the fullest extent permitted by Data Protection Laws.

**10. Cross-Border Transfers/Region-Specific Terms.**

- 10.1. Cross-Border Data Transfers.
  - (a) Provider (and its Affiliates) may Process and transfer Customer Personal Data globally as necessary to provide the Cloud Service.
  - (b) If Provider engages in a Restricted Transfer, it will comply with Schedule 3 (Cross-Border Transfer Mechanisms).
- 10.2. Region-Specific Terms. To the extent that Provider Processes Customer Personal Data protected by Data Protection Laws in one of the regions listed in Schedule 4 (Region-Specific Terms), then the terms specified therein with respect to the applicable jurisdiction(s) will apply in addition to the terms of this DPA.

**Schedule 1: Subject Matter and Details of Processing**

**Customer / ‘Data Exporter’ Details**

<b>Name:</b>	<b>Customer, as specified in the Order Form.</b>
--------------	--



	<p>In accordance with the timeframes specified in the Agreement, Processor will securely destroy (in accordance with standard industry practices for deletion of personal data) all copies of Controller’s personal data.</p> <p>Upon Controller’s request, Processor will promptly deliver to Controller an export of Controller’s personal data (in CSV or similar format) within thirty (30) calendar days and, if Customer also requests deletion of Controller’s personal data, will carry that out as set forth above.</p> <p>Tapes, printed output, optical disks, and other physical media will be physically destroyed by a secure method and by a recognized provider.</p>
<p><b>Transfers to Subprocessors:</b></p>	<p>Standard Contractual Clauses approved by the European Commission Decision of 4 June 2021 (as amended from time to time), for the transfer of personal data from the EEA or adequate country to a third country.</p> <p>International Data Transfer Addendum issued by the United Kingdom’s Information Commissioner’s Office under Section 119A of the Data Protection Act 2018, effective from 21 March 2022.</p>

## Schedule 2: Technical and Organizational Measures

Please visit <https://contractpodai.com/resources/security-information-datasheet/> for the latest Provider security information datasheet. Provider may modify the Security Information Datasheet or Provider’s information security and privacy measures to reflect new technical and organizational measures or changing practices, but the modifications may not be retroactive or materially decrease Provider’s overall obligations during a Subscription Term.

## Schedule 3: Cross-Border Transfer Mechanisms

1. **Definitions.** Capitalized terms not defined in this Schedule are defined in the DPA.
  - 1.1. **“EU Standard Contractual Clauses”** or **“EU SCCs”** means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.
  - 1.2. **“UK International Data Transfer Agreement”** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force as of March 21, 2022.
  - 1.3. In addition:

<p><b>“Designated EU Governing Law”</b> means:</p>	<p>Republic of Ireland</p>
<p><b>“Designated EU Member State”</b> means:</p>	<p>Republic of Ireland</p>

2. **EU Transfers.** Where Customer Personal Data is protected by EU GDPR and is subject to a Restricted Transfer, the following applies:
  - 2.1. The EU SCCs are hereby incorporated by reference as follows:
    - (a) Module 2 (Controller to Processor) applies where Customer is a Controller of Customer Personal Data and Provider is a Processor of Customer Personal Data;
    - (b) Module 3 (Processor to Processor) applies where Customer is a Processor of Customer Personal Data (on behalf of a third-party Controller) and Provider is a Processor of Customer Personal Data;
    - (c) Customer is the "data exporter" and Provider is the "data importer"; and
    - (d) by entering into this DPA, each party is deemed to have signed the EU SCCs (including their Annexes) as of the DPA Effective Date.
  - 2.2. For each Module, where applicable the following applies:
    - (a) the optional docking clause in Clause 7 does not apply;
    - (b) in Clause 9, Option 2 will apply, the minimum time period for prior notice of Subprocessor changes shall be as set out in Section 4.3 of this DPA, and Provider shall fulfill its notification obligations by notifying Customer of any Subprocessor changes in



accordance with Section 4.3 of this DPA;

- (c) in Clause 11, the optional language does not apply;
- (d) in Clause 13, all square brackets are removed with the text remaining;
- (e) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Designated EU Governing Law;
- (f) in Clause 18(b), disputes will be resolved before the courts of the Designated EU Member State;
- (g) Schedule 1 (Subject Matter and Details of Processing) to this DPA contains the information required in Annex 1 of the EU SCCs; and
- (h) Schedule 2 (Technical and Organizational Measures) to this DPA contains the information required in Annex 2 of the EU SCCs.

2.3. Where context permits and requires, any reference in this DPA to the EU SCCs shall be read as a reference to the EU SCCs as modified in the manner set forth in this Section 2.

3. **Swiss Transfers.** Where Customer Personal Data is protected by the FADP and is subject to a Restricted Transfer, the following applies:

3.1. The EU SCCs apply as set forth in Section 2 (EU Transfers) of this Schedule 3 with the following modifications:

- (a) in Clause 13, the competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner;
- (b) in Clause 17 (Option 1), the EU SCCs will be governed by the laws of Switzerland;
- (c) in Clause 18(b), disputes will be resolved before the courts of Switzerland;
- (d) the term Member State must not be interpreted in such a way as to exclude Data Subjects in Switzerland from enforcing their rights in their place of habitual residence in accordance with Clause 18(c); and
- (e) all references to the EU GDPR in this DPA are also deemed to refer to the FADP.

4. **UK Transfers.** Where Customer Personal Data is protected by the UK GDPR and is subject to a Restricted Transfer, the following applies:

4.1. The EU SCCs apply as set forth in Section 2 (EU Transfers) of this Schedule 3 with the following modifications:

- (a) each party shall be deemed to have signed the “UK Addendum to the EU Standard Contractual Clauses” (“**UK Addendum**”) issued by the Information Commissioner’s Office under section 119 (A) of the Data Protection Act 2018;
- (b) the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of Customer Personal Data;
- (c) in Table 1 of the UK Addendum, the parties’ key contact information is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA;
- (d) in Table 2 of the UK Addendum, information about the version of the EU SCCs, modules and selected clauses which this UK Addendum is appended to are located above in this Schedule 3;
- (e) in Table 3 of the UK Addendum:
  - (i) the list of parties is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA;
  - (ii) the description of transfer is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA;
  - (iii) Annex II is located in Schedule 2 (Technical and Organizational Measures) to this DPA; and
  - (iv) the list of Subprocessors is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA.
- (f) in Table 4 of the UK Addendum, both the Importer and the Exporter may end the UK Addendum in accordance with its terms (and the respective box for each is deemed checked); and
- (g) in Part 2: 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 section 119 (A) of the Data Protection Act 2018 on 2 February 2022, as it is revised under section 18 of those Mandatory Clauses.

## Schedule 4: Region-Specific Terms

### California

1. **Definitions.** CCPA and other capitalized terms not defined in this Schedule are defined in the DPA.

- 1.1. “business purpose”, “commercial purpose”, “personal information”, “sell”, “service provider” and “share” have the meanings given in the CCPA.
- 1.2. The definition of “Data Subject” includes “consumer” as defined under the CCPA.
- 1.3. The definition of “Controller” includes “business” as defined under the CCPA.

1.4. The definition of “Processor” includes “service provider” as defined under the CCPA.

## 2. Obligations.

- 2.1. Customer is providing the Customer Personal Data to Provider under the Agreement for the limited and specific business purposes of providing the Cloud Service as described in Schedule 1 (Subject Matter and Details of Processing) to this DPA and otherwise performing under the Agreement.
- 2.2. Provider will comply with its applicable obligations under the CCPA and provide the same level of privacy protection to Customer Personal Data as is required by the CCPA.
- 2.3. Provider acknowledges that Customer has the right to: (i) take reasonable and appropriate steps under Section 9 (Audits) of this DPA to help to ensure that Provider’s use of Customer Personal Data is consistent with Customer’s obligations under the CCPA, (ii) receive from Provider notice and assistance under Section 7 (Data Subject Requests) of this DPA regarding consumers’ requests to exercise rights under the CCPA and (iii) upon notice, take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Data.
- 2.4. Provider will notify Customer promptly after it makes a determination that it can no longer meet its obligations under the CCPA.
- 2.5. Provider will not retain, use or disclose Customer Personal Data: (i) for any purpose, including a commercial purpose, other than the business purposes described in Section 2.1 of this Section A (California) of Schedule 4 or (ii) outside of the direct business relationship between Provider with Customer, except, in either case, where and to the extent permitted by the CCPA.
- 2.6. Provider will not sell or share Customer Personal Data received under the Agreement.
- 2.7. Provider will not combine Customer Personal Data with other personal information except to the extent a service provider is permitted to do so by the CCPA.

**Activity Prior to January 1, 2023.** To the extent this Section A (California) of Schedule 4 is in effect prior to January 1, 2023, Provider’s obligations hereunder that are required solely by amendments to the CCPA made by the California Privacy Rights Act regarding contractual obligations of service providers shall only apply on and after January 1, 2023.