ContractPodAi Master Terms & Annexes

THE EXPLAINER: WHY CONTRACTPODAI USES BONTERMS CLOUD TERMS AND ONEDPA

We appreciate the chance to explain why **ContractPodAi** has chosen to use the **Bonterms Cloud Terms** and **oneDPA** to be the perfect starting point for working together.

Why Bonterms Cloud Terms? The Cloud Terms are designed to be **a neutral starting point** for an agreement that meets the needs of both ContractPodAi and enterprise customers (like you!).

We recognize that there might be some needed changes — so we ask that we work together to make the changes on the Cover Page / Order Form and not hidden in the full set of ContractPodAi Master Terms. This means we can skip the battle over whose form to use, preserve goodwill, and move straight to negotiating the issues that we both really care about (and where there is a special concern, both parties are fully aware, since it is on the Cover Page / Order Form)!

Why oneDPA? Data processing agreements are long, extensive, and an unfortunate necessity in the world today. The **oneDPA** project allows us to have a standard, recognizable, and easily adoptable DPA that can be quickly understood and easily reviewed (and all with neutral positions that allow both you and ContractPodAi to move through understanding how we protect your trusted data and information.

Both Bonterms and oneDPA are **best-practice**, **balanced,** and **open source**:

- **Best-practice?**
  - The Bonterms Cloud Terms were drafted and extensively reviewed and revised by a 40-member Open Source Forms Committee of in-house and law firm lawyers. They took the task seriously. The Cloud Terms went through six major drafts, three sub-committees (Data, Risk and General Terms) and multiple meetings, surveys and discussions across seven months.
  - The oneDPA was drafted with input from 25+ members of the oneDPA SteerCo (and with input from over 1000 practitioners), including some of the world's most recognizable brands and law firms. Over the course of three months and countless drafts, the oneDPA SteerCo created a module-based DPA that can be used by controllers and processors throughout the world.
- **Balanced?** Both oneDPA and the Bonterms Cloud Terms are designed to meet the needs of both parties and not inherently favor either.
- **Open source?** The Bonterms Cloud Terms and the oneDPA are free to use under CC BY 4.0.

The entire ContractPodAi team is excited to get you up-and-running on our award-winning solution. It is our hope that adopting these balanced, open-source, and best-practice documents will expedite your legal department's digital transformation and empower in-house legal professionals to optimize operational workflows, increase compliance adherence, and drive quicker revenue recognition.

THE TERMS GOVERNING YOUR USE OF THE CONTRACTPODAI SERVICES.

Please note that, rather than modifying these Master Terms — and to make things clear and understandable where there are changes — modifications (if any) should be recorded & addressed in the Cover Page / Order Form. We do this to ensure that all people involved in delivering our solution and providing your order are aware of your specific needs.

THE APPLICABLE TERMS	WHAT THEY DO
The **Bonterms Cloud Terms v1**[1]	Contain the core legal and commercial terms that apply to your subscription
ContractPodAi's **Support Policy** and **Service Level Agreement**	Details how our support services function
oneDPA[2] **(Data Processing Addendum)**	Explains how your personal data should be processed
ContractPodAi's **Acceptable Use Policy**	Describes what you may and may not do when accessing our cloud service.
Your Cover Page / Order Form and **Statement of Work**	Contain the details of your purchase, including your subscription term, the products to which you have subscribed, the details of any purchases, your fees, the implementation plan, and other important order-related information.

[1] These terms are identical to the publicly available Bonterms Cloud Terms V1, which is released under CC-BY-4.0.

[2] ContractPodAi is proudly a sponsor of the oneDPA project to bring standardization and ease of use to data processing agreements.

Table of contents

MAIN AGREEMENT: BONTERMS CLOUD TERMS (V. 1.0)[3]

1. The Agreement.

The Bonterms Cloud Terms are standardized terms for use of cloud services. To use the Bonterms Cloud Terms, Customer and Provider complete and execute a Cover Page that specifies Key Terms, Attachments (such as a Support Policy or Data Protection Addendum) and any Additional Terms. Collectively, the Bonterms Cloud Terms, Cover Page and any Orders form the parties' agreement ("**Agreement**"). Conflicts between parts of the Agreement are governed by Section 22.5 (Order of Precedence). Capitalized terms are defined in context or in the Definitions section.

2. Cloud Service.

Subject to this Agreement, Customer may use the Cloud Service for its own business purposes during each Subscription Term ("**Permitted Use**"). This includes the right to copy and use the Provider Software (if any) and Documentation as part of Customer's Permitted Use. Customer will comply with the Documentation in using the Cloud Service.

3. Users

Customer may permit Users to use the Cloud Service on its behalf. Customer is responsible for provisioning and managing its User accounts, for its Users' actions through the Cloud Service and for their compliance with this Agreement. Customer will ensure that Users keep their login credentials confidential and will promptly notify Provider upon learning of any compromise of User accounts or credentials.

4. Affiliates

Customer's Affiliates may serve as Users under this Agreement. Alternatively, Customer's Affiliates may enter into their own Orders as mutually agreed with Provider, which creates a separate agreement between each such Affiliate and Provider incorporating this Agreement with the Affiliate treated as "Customer". Neither Customer nor any Customer Affiliate has any rights under each other's separate agreement with Provider, and breach or termination of any such separate agreement affects only that agreement.

5. Data.

5.1 **Use of Customer Data.** Subject to this Agreement, Provider will access and use Customer Data solely to provide and maintain the Cloud Service, Support and Professional Services under this Agreement ("Use of Customer Data"). Use of Customer Data includes sharing Customer Data as Customer directs through the Cloud Service, but Provider will not otherwise disclose Customer Data to third parties except as permitted in this Agreement.

5.2 **Security.** Provider will implement and maintain the **Security Measures** identified on the Cover Page. If no Security Measures are identified, Provider will use appropriate technical and organizational measures designed to prevent unauthorized access, use, alteration or disclosure of Customer Data.

5.3 **DPA.** The parties will adhere to the **Data Protection Addendum** (**DPA**), if any, identified on the Cover Page.

5.4 **Usage Data**. Provider may collect Usage Data and use it to operate, improve and support the Cloud Service and for other lawful business purposes, including benchmarking and reports. However, Provider will not disclose Usage Data externally unless it is (a) de-identified so that it does not identify Customer, its Users or any other person and (b) aggregated with data across other customers.

6. Mutual Compliance with Laws.

Each party will comply with all Laws that apply to its performance under this Agreement.

[3] As noted above, these terms are identical to the publicly available Bonterms Cloud Terms V1, which is released under CC-BY-4.0.

7. Support and SLA.

7.1 **Support**. Provider will provide Support for the Cloud Service as described in the **Support Policy** on the Cover Page. If no Support Policy is identified, Provider will provide Support for the Cloud Service consistent with industry-standards and its general business practices.

7.2 **SLA**. Provider will adhere to the **Service Level Agreement (SLA)** identified on the Cover Page. If no SLA is identified, Provider will use commercially reasonable efforts to make the Cloud Service available for Customer's use 99.9% of the time in each month.

8. Warranties.

8.1 **Mutual Warranties.** Each party represents and warrants that:

(a) it has the legal power and authority to enter into this Agreement, and

(b) it will use industry-standard measures to avoid introducing Viruses into the Cloud Service.

8.2 **Additional Provider Warranties**. Provider warrants that:

(a) the Cloud Service will perform materially as described in the Documentation and Provider will not materially decrease the overall functionality of the Cloud Service during a Subscription Term (the "**Performance Warranty**"), and

(b) any Professional Services will be provided in a professional and workmanlike manner (the "**Professional Services Warranty**").

8.3 **Warranty Remedy**. Provider will use reasonable efforts to correct a verified breach of the Performance Warranty or Professional Services Warranty reported by Customer. If Provider fails to do so within 30 days after Customer's warranty report ("**Fix Period**"), then either party may terminate the Order as relates to the non-conforming Cloud Service or Professional Services, in which case Provider will refund to Customer any pre-paid, unused fees for the terminated portion of the Subscription Term (for the Performance Warranty) or for the non-conforming Professional Services (for the Professional Services Warranty). To receive these remedies, Customer must report a breach of warranty in reasonable detail within 30 days after discovering the issue in the Cloud Service or 30 days after delivery of the relevant Professional Services ("**Claim Period**"). These procedures are Customer's exclusive remedies and Provider's sole liability for breach of the Performance Warranty or Professional Services Warranty.

8.4 **Disclaimers**. **Except as expressly set out in this Agreement, each party disclaims all warranties, whether express, implied, statutory or otherwise, including warranties of merchantability, fitness for a particular purpose, title and noninfringement. Provider's warranties in this Section 8 do not apply to issues arising from Third Party Platforms or misuse or unauthorized modifications of the Cloud Service. These disclaimers apply to the full extent permitted by Law.**

9. Usage Rules

9.1 **Compliance**. Customer (a) will comply with any **Acceptable Use Policy (AUP)** identified on the Cover Page and (b) represents and warrants that it has all rights necessary to use Customer Data with the Cloud Service and grant Provider the rights to Customer Data specified in this Agreement, without violating third-party intellectual property, privacy or other rights. Between the parties, Customer is responsible for the content and accuracy of Customer Data.

9.2 **High Risk Activities & Sensitive Data.** Customer will not (a) use the Cloud Service for High Risk Activities, (b) will not submit Sensitive Data to the Cloud Service, and acknowledges that the Cloud Service is not designed for (and Provider has no liability for) use prohibited in this Section 9.2.

9.3 **Restrictions.** Customer will not and will not permit anyone else to: (a) sell, sublicense, distribute or rent the Cloud Service (in whole or part), grant non-Users access to the Cloud Service or use the Cloud Service to provide a hosted or managed service to others, (b) reverse engineer, decompile or seek to access the source code of the Cloud Service, except to the extent these restrictions are prohibited by Laws and then only upon advance notice to Provider, (c) copy, modify, create derivative works of or remove proprietary notices from the Cloud Service, (d) conduct security or vulnerability tests of the Cloud Service, interfere with its operation or circumvent its access restrictions or (e) use the Cloud Service to develop a product that competes with the Cloud Service.

10. Third-Party Platforms.

Customer may choose to enable integrations or exchange Customer Data with Third-Party Platforms. Customer's use of a Third-Party Platform is governed by its agreement with the relevant provider, not this Agreement, and Provider is not responsible for Third-Party Platforms or how their providers use Customer Data.

11. Professional Services.

Provider will perform Professional Services as described in an Order or Statement of Work, which may identify additional terms or milestones for the Professional Services. Customer will give Provider timely access to Customer Materials reasonably needed for Professional Services, and Provider will use the Customer Materials only for purposes of providing Professional Services. Subject to any limits in an Order or Statement of Work, Customer will reimburse Provider's reasonable travel and lodging expenses incurred in providing Professional Services. Customer may use code or other deliverables that Provider furnishes as part of Professional Services only in connection with Customer's authorized use of the Cloud Service under this Agreement.

12. Fees.

12.1 **Payment.** Customer will pay the fees described in the Order. Unless the Order states otherwise, all amounts are due within 30 days after the invoice date (the "**Payment Period**"). Late payments are subject to a charge of 1.5% per month or the maximum amount allowed by Law, whichever is less. All fees and expenses are non-refundable except as expressly set out in this Agreement.

12.2 **Taxes**. Customer is responsible for any sales, use, GST, value-added, withholding or similar taxes or levies that apply to its Orders, whether domestic or foreign ("**Taxes**"), other than Provider's income tax. Fees and expenses are exclusive of Taxes.

12.3 **Payment Disputes.** If Customer disputes an invoice in good faith, it will notify Provider within the Payment Period and the parties will seek to resolve the dispute over a 15-day discussion period. Customer is not required to pay disputed amounts during the discussion period, but will timely pay all undisputed amounts. After the discussion period, either party may pursue any available remedies.

13. Suspension.

Provider may suspend Customer's access to the Cloud Service and related services due to a Suspension Event, but where practicable will give Customer prior notice so that Customer may seek to resolve the issue and avoid suspension. Provider is not required to give prior notice in exigent circumstances or for a suspension made to avoid material harm or violation of Law. Once the Suspension Event is resolved, Provider will promptly restore Customer's access to the Cloud Service in accordance with this Agreement. "**Suspension Event**" means (a) Customer's account is 30 days or more overdue, (b) Customer is in breach of Section 9 (Usage Rules) or (c) Customer's use of the Cloud Service risks material harm to the Cloud Service or others.

14. Term and Termination.

14.1 **Subscription Terms.** Each **Subscription Term** will last for an initial 12-month period unless the Order states otherwise. Each Subscription Term will renew for successive periods unless (a) the parties agree on a different renewal Order or (b) either party notifies the other of non-renewal at least 30 days prior to the end of the current Subscription Term.

14.2 **Term of Agreement.** This Agreement starts on the **Effective Date** and continues until the end of all Subscription Terms, unless sooner terminated in accordance with its terms. If no Subscription Term is in effect, either party may terminate this Agreement for any or no reason with notice to the other party.

14.3 **Termination**. Either party may terminate this Agreement (including all Subscription Terms) if the other party (a) fails to cure a material breach of this Agreement within 30 days after notice, (b) ceases operation without a successor or (c) seeks protection under a bankruptcy, receivership, trust deed, creditors' arrangement, composition or comparable proceeding, or if such a proceeding is instituted against that party and not dismissed within 60 days.

14.4 **Data Export & Deletion.**

During a Subscription Term, Customer may export Customer Data from the Cloud Service (or Provider will otherwise make the Customer Data available to Customer) as described in the Documentation.

After termination or expiration of this Agreement, within 60 days of request, Provider will delete Customer Data and each party will delete any Confidential Information of the other in its possession or control.

Nonetheless, the recipient may retain Customer Data or Confidential Information in accordance with its standard backup or record retention policies or as required by Law, subject to Section 5.2 (Security), Section 18 (Confidentiality) and any DPA.

14.5 Effect of Termination.

(a) Customer's right to use the Cloud Service, Support and Professional Services will cease upon any termination or expiration of this Agreement, subject to this Section 14.

(b) The following Sections will survive expiration or termination of this Agreement: 5.4 (Usage Data), 8.4 (Disclaimers), 9 (Usage Rules), 12.1 (Payment) (for amounts then due), 12.2 (Taxes), 14.4 (Data Export & Deletion), 14.5 (Effect of Termination), 15 (Intellectual Property), 16 (Limitations of Liability), 17 (Indemnification), 18 (Confidentiality), 19 (Required Disclosures), 22 (General Terms) and 23 (Definitions).

(c) Except where an exclusive remedy is provided, exercising a remedy under this Agreement, including termination, does not limit other remedies a party may have.

15. Intellectual Property.

15.1 Reserved Rights. Neither party grants the other any rights or licenses not expressly set out in this Agreement. Except for Provider's express rights in this Agreement, as between the parties, Customer retains all intellectual property and other rights in Customer Data and Customer Materials provided to Provider. Except for Customer's express rights in this Agreement, as between the parties, Provider and its licensors retain all intellectual property and other rights in the Cloud Service, Professional Services deliverables and related Provider technology.

15.2 Feedback. If Customer gives Provider feedback regarding improvement or operation of the Cloud Service, Support or Professional Services, Provider may use the feedback without restriction or obligation. All feedback is provided "AS IS" and Provider will not publicly identify Customer as the source of feedback without Customer's permission.

16. Limitations of Liability.

16.1 General Cap. Each party's entire liability arising out of or related to this Agreement will not exceed the General Cap.

16.2 Consequential Damages Waiver. Neither party will have any liability arising out of or related to this Agreement for indirect, special, incidental, reliance or consequential damages or damages for loss of use, lost profits or interruption of business, even if informed of their possibility in advance.

16.3 Exceptions and Enhanced Cap. Sections 16.1 (General Cap) and 16.2 (Consequential Damages Waiver) will not apply to Enhanced Claims or Uncapped Claims. For all Enhanced Claims, each party's entire liability will not exceed the Enhanced Cap.

16.4 Nature of Claims. The waivers and limitations in this Section 16 apply regardless of the form of action, whether in contract, tort (including negligence), strict liability or otherwise and will survive and apply even if any limited remedy in this Agreement fails of its essential purpose.

16.5 Liability Definitions. The following definitions apply unless modified on the Cover Page.

"Enhanced Cap" means three times (3x) the General Cap.

"Enhanced Claims" means Provider's breach of Section 5.2 (Security) or either party's breach of Section 5.3 (DPA).

"General Cap" means amounts paid or payable by Customer to Provider under this Agreement in the 12 months immediately preceding the first incident giving rise to liability.

"Uncapped Claims" means (a) the indemnifying party's obligations under Section 17 (Indemnification), (b) either party's infringement or misappropriation of the other party's intellectual property rights, (c) any breach of Section 18 (Confidentiality), excluding breaches related to Customer Data and (d) liabilities that cannot be limited by Law.

17. Indemnification.

17.1 Indemnification by Provider. Provider, at its own cost, will defend Customer from and against any Provider-Covered Claims and will indemnify and hold harmless Customer from and against any damages or costs awarded against Customer (including reasonable attorneys' fees) or agreed in settlement by Provider resulting from the Provider-Covered Claims.

17.2 Indemnification by Customer. Customer, at its own cost, will defend Provider from and against any Customer-Covered Claims and will indemnify and hold harmless Provider from and against any damages or costs awarded against Provider (including reasonable attorneys' fees) or agreed in settlement by Customer resulting from the Customer-Covered Claims.

17.3 Indemnification Definitions.

The following definitions apply unless modified on the Cover Page.

"**Customer-Covered Claim**" means a third-party claim arising from Customer's breach or alleged breach of Section 9.1 (Compliance) or 9.2 (High-Risk Activities & Sensitive Data).

"**Provider-Covered Claim**" means a third-party claim that the Cloud Service, when used by Customer as authorized in this Agreement, infringes or misappropriates a third party's intellectual property rights.

17.4 Procedures.

The indemnifying party's obligations in this Section are subject to receiving from the indemnified party: (a) prompt notice of the claim (but delayed notice will only reduce the indemnifying party's obligations to the extent it is prejudiced by the delay), (b) the exclusive right to control the claim's investigation, defense and settlement and (c) reasonable cooperation at the indemnifying party's expense. The indemnifying party may not settle a claim without the indemnified party's prior approval if settlement would require the indemnified party to admit fault or take or refrain from taking any action (except regarding use of the Cloud Service when Provider is the indemnifying party). The indemnified party may participate in a claim with its own counsel at its own expense.

17.5 Mitigation.

In response to an infringement or misappropriation claim, if required by settlement or injunction or as Provider determines necessary to avoid material liability, Provider may: (a) procure rights for Customer's continued use of the Cloud Service, (b) replace or modify the allegedly infringing portion of the Cloud Service to avoid infringement, without reducing the Cloud Service's overall functionality or (c) terminate the affected Order and refund to Customer any pre-paid, unused fees for the terminated portion of the Subscription Term.

17.6 Exceptions.

Provider's obligations in this Section 17 do not apply to claims resulting from (a) modification or unauthorized use of the Cloud Service, (b) use of the Cloud Service in combination with items not provided by Provider, including Third-Party Platforms or (c) Provider Software other than the most recent release, if Provider made available (at no additional charge) a newer release that would avoid infringement.

17.7 Exclusive Remedy.

This Section sets out the indemnified party's exclusive remedy and the indemnifying party's sole liability regarding third-party claims of intellectual property infringement or misappropriation covered by this Section 17.

18. Confidentiality.

18.1 Use and Protection.

As recipient, each party will (a) use Confidential Information only to fulfill its obligations and exercise its rights under this Agreement, (b) not disclose Confidential Information to third parties without the discloser's prior approval, except as permitted in this Agreement and (c) protect Confidential Information using at least the same precautions recipient uses for its own similar information and no less than a reasonable standard of care.

18.2 Permitted Disclosures.

The recipient may disclose Confidential Information to its employees, agents, contractors and other representatives having a legitimate need to know (including, for Provider, the subcontractors referenced in Section 22.10), provided it remains responsible for their compliance with this Section 18 and they are bound to confidentiality obligations no less protective than this Section 18.

18.3 Exclusions.

These confidentiality obligations do not apply to information that the recipient can document (a) is or becomes public knowledge through no fault of the recipient, (b) it rightfully knew or possessed, without confidentiality restrictions, prior to receipt from the discloser, (c) it rightfully received from a third party without confidentiality restrictions or (d) it independently developed without using or referencing Confidential Information.

18.4 Remedies.

Breach of this Section 18 may cause substantial harm for which monetary damages are an insufficient remedy. Upon a breach of this Section, the discloser is entitled to seek appropriate equitable relief, including an injunction, in addition to other remedies.

19. Required Disclosures.

The recipient may disclose Confidential Information (including Customer Data) to the extent required by Laws. If permitted by Law, the recipient will give the discloser reasonable advance notice of the required disclosure and reasonably cooperate, at the discloser's expense, to obtain confidential treatment for the Confidential Information.

20. Publicity.

Neither party may publicly announce this Agreement without the other party's prior approval or except as required by Laws.

21. Trials and Betas.

Provider may offer optional Trials and Betas. Use of Trials and Betas is permitted only for Customer's internal evaluation during the period designated by Provider on the Order (or if not designated, 30 days). Either party may terminate Customer's use of Trials and Betas at any time for any reason. Trials and Betas may be inoperable, incomplete or include features never released. **Notwithstanding anything else in this Agreement, Provider offers no warranty, indemnity, SLA or Support for Trials and Betas and its liability for Trials and Betas will not exceed US$1,000**.

22. General Terms.

22.1 Assignment.

Neither party may assign this Agreement without the prior consent of the other party, except that either party may assign this Agreement, with notice to the other party, in connection with the assigning party's merger, reorganization, acquisition or other transfer of all or substantially all of its assets or voting securities. Any non-permitted assignment is void. This Agreement will bind and inure to the benefit of each party's permitted successors and assigns.

22.2 Governing Law and Courts.

The **Governing Law** governs this Agreement and any action arising out of or relating to this Agreement, without reference to conflict of law rules. The parties will adjudicate any such action in the **Courts** and each party consents to the exclusive jurisdiction and venue of the **Courts** for these purposes.

22.3 Notices.

Except as set out in this Agreement, notices, requests and approvals under this Agreement must be in writing to the addresses on the Cover Page and will be deemed given: (1) upon receipt if by personal delivery, (2) upon receipt if by certified or registered U.S. mail (return receipt requested), (3) one day after dispatch if by a commercial overnight delivery or (4) upon delivery if by email. Either party may update its address with notice to the other.

Provider may also send operational notices through the Cloud Service.

22.4 Entire Agreement.

This Agreement is the parties' entire agreement regarding its subject matter and supersedes any prior or contemporaneous agreements regarding its subject matter. In this Agreement, headings are for convenience only and "including" and similar terms are to be construed without limitation. Excluding Orders, terms in business forms, purchase orders or quotes used by either party will not amend or modify this Agreement; any such documents are for administrative purposes only. This Agreement may be executed in counterparts (including electronic copies and PDFs), each of which is deemed an original and which together form one and the same agreement.

22.5 Order of Precedence.

First any Additional Terms and then Attachments will control in any conflict with these Bonterms Cloud Terms. An Order may not modify any other part of the Agreement unless the Order specifically identifies the provisions that it supersedes.

22.6 Amendments.

Any amendments to this Agreement must be in writing and signed by each party's authorized representatives.

22.7 Operational Changes.

With notice to Customer, Provider may modify the **Support Policy, SLA** or **Security Measures** to reflect new features or changing practices, but the modifications may not be retroactive or materially decrease Provider's overall obligations during a Subscription Term.

22.8 Waivers and Severability.

Waivers must be signed by the waiving party's authorized representative and cannot be implied from conduct. If any provision of this Agreement is held invalid, illegal or unenforceable, it will be limited to the minimum extent necessary so the rest of this Agreement remains in effect.

22.9 Force Majeure.

Neither party is liable for a delay or failure to perform this Agreement due to a Force Majeure. If a Force Majeure materially adversely affects the Cloud Service for 15 or more consecutive days, either party may terminate the affected Order(s) upon notice to the other and Provider will refund to Customer any pre-paid, unused fees for the terminated portion of the Subscription Term. However, this Section does not limit Customer's obligations to pay fees owed.

22.10 Subcontractors.

Provider may use subcontractors and permit them to exercise its rights and fulfill its obligations, but Provider remains responsible for their compliance with this Agreement and for its overall performance under this Agreement. This does not limit any additional terms for subprocessors under a DPA.

22.11 Independent Contractors.

The parties are independent contractors, not agents, partners or joint venturers.

22.12 No Third-Party Beneficiaries.

There are no third-party beneficiaries to this Agreement.

22.13 Open Source.

Provider Software distributed to Customer (if any) may include third-party open source software ("**Open Source**") as listed in the Documentation or by Provider upon request. If Customer elects to use the Open Source on a stand-alone basis, that use is subject to the applicable Open Source license and not this Agreement.

22.14 Export.

Each party (a) will comply with all export and import Laws in performing this Agreement and (b) represents and warrants that it is not listed on any U.S. government list of prohibited or restricted parties or located in (or a national of) a country subject to a U.S. government embargo or designated by the U.S. government as a "terrorist supporting" country. Customer will not submit to the Cloud Service any data controlled under the U.S. International Traffic in Arms Regulations.

22.15 Government Rights.

To the extent applicable, the Cloud Service is "commercial computer software" or a "commercial item" for purposes of FAR 12.212 for and DFARS 227.7202. Use, reproduction, release, modification, disclosure or transfer of the Cloud Service is governed solely by the terms of this Agreement, and all other use is prohibited.

23. Definitions.

"Acceptable Use Policy" or "AUP" is defined in Section 9.1 (Compliance).	**"Additional Terms"** means any additions to or modifications of these Bonterms Cloud Terms that the parties specify on the Cover Page.
"Affiliate" means an entity controlled, controlling or under common control with a party, where control means at least 50% ownership or power to direct an entity's management.	**"Agreement"** has the meaning given in Section 1 (The Agreement).
"Attachments" means any attachments, policies or documents that the parties specify on the Cover Page.	**"Bonterms Cloud Terms"** means these Bonterms Cloud Terms (Version 1.0).
"**Cloud Service**" means Provider's proprietary cloud service, as identified in the relevant Order and as modified from time to time. The Cloud Service includes the Provider Software and Documentation but not Professional Services deliverables or Third-Party Platforms.	**"Confidential Information"** means information disclosed by or on behalf of one party (as discloser) to the other party (as recipient) under this Agreement, in any form, which (a) the discloser identifies to recipient as "confidential" or "proprietary" or (b) should be reasonably understood as confidential or proprietary due to its nature and the circumstances of its disclosure. Provider's Confidential Information includes technical or performance information about the Cloud Service, and Customer's Confidential Information includes Customer Data. Information on the Cover Page is each party's Confidential Information.
"Cover Page" means a Bonterms cover page or other document that (a) incorporates these Bonterms Cloud Terms by reference, (b) specifies the Key Terms and any Additional Terms and incorporates any Attachments and (c) is signed by Customer and Provider.	**"Customer"** means the party identified as "Customer" on the Cover Page.
"Customer Data" means any data, content or materials that Customer (including its Users) submits to its Cloud Service accounts, including from Third-Party Platforms.	**"Customer Materials"** means materials and resources that Customer makes available to Provider in connection with Professional Services.
"Data Protection Addendum" or "DPA" is defined in Section 5.3 (DPA).	**"Documentation"** means Provider's standard usage documentation for the Cloud Service.
"Force Majeure" means an unforeseen event beyond a party's reasonable control, such as a strike, blockade, war, pandemic, act of terrorism, riot, third-party Internet or utility failure, refusal of government license or natural disaster, where the affected party takes reasonable and customary measures to avoid or mitigate such event's effects.	**"High Risk Activities"** means activities where use or failure of the Cloud Service could lead to death, personal injury or environmental damage, including life support systems, emergency services, nuclear facilities, autonomous vehicles or air traffic control.
"Key Terms" means Effective Date, Governing Law, Courts or other terms specified by the parties as "Key Terms" on the Cover Page.	**"Laws"** means all laws, regulations, rules, court orders or other binding requirements of a government authority that apply to a party.

"Order" means an order for Customer's access to the Cloud Service, Support, Professional Services or related services that is executed by the parties and references this Agreement.	**"Personal Data"** means Customer Data relating to an identified or identifiable natural person.
"Professional Services" means training, migration or other professional services that Provider furnishes to Customer related to the Cloud Service.	**"Provider"** means the party identified as "Provider" on the Cover Page.
"Provider Software" means any proprietary apps or software that Provider distributes to Customer as part of the Cloud Service.	**"Sensitive Data"** means (a) patient, medical or other protected health information regulated by the Health Insurance Portability and Accountability Act (as amended and supplemented) ("HIPAA"), (b) credit, debit, bank account or other financial account numbers, (c) social security numbers, driver's license numbers or other government ID numbers and (d) special categories of data enumerated in European Union Regulation 2016/679, Article 9(1) or any successor legislation.
"Service Level Agreement" or "SLA" is defined in Section 7.2 (SLA).	**"Statement of Work"** means a statement of work for Professional Services that is executed by the parties and references this Agreement.
"Subscription Term" means the term for Customer's use of the Cloud Service as identified in an Order.	**"Support"** means support for the Cloud Service as described in Section 7.1 (Support).
"**Support Policy"** is defined in Section 7.1 (Support).	**"Third-Party Platform"** means any product, add-on or platform not provided by Provider that Customer uses with the Cloud Service.
"Trials and Betas" mean access to the Cloud Service (or Cloud Service features) on a free, trial, beta or early access basis.	**"Usage Data"** means Provider's technical logs, data and learnings about Customer's use of the Cloud Service, but excluding Customer Data.
"User" means anyone that Customer allows to use its accounts for the Cloud Service, who may include (a) employees, advisors and contractors of Customer and its Affiliates and (b) others if permitted in this Agreement, the Documentation or an Order.	**"Virus"** means viruses, malicious code or similar harmful materials.

ANNEX A: CONTRACTPODAI'S SUPPORT POLICY AND SERVICE LEVEL AGREEMENT

Introduction & Definitions

Subject to the Agreement and payment of your Subscription Fees, we will allow you to access and use the Cloud Service and receive the Support Services specified in this Annex A.

If we use a capitalized term in this Support and Service Level Policy—and it is not defined otherwise in this Support and Service Level Policy—then it has the same meaning as in the Master Terms. The following are additional definitions:

"Service Failure" means a verifiable failure of the Cloud Service that you have demonstrated or documented to us.

"Support Request" means a request for support that is not related to a Service Failure.

"Support Services" means the applicable support services described in this Service Level Policy.

"Target Resolution Time" means the estimated time to resolve a Service Failure.

Scope of Support Services

Responding to Support Requests

You will have a designated Customer Success Manager who you can contact for Support Requests. Their contact information will be shared with you.

You may also send a Support Request to our general Customer Support mailbox (support@contractpodai.com) or access other resources that we may make available for assistance with the Cloud Service.

Depending on the nature and scope of the Support Request, we may classify it as an upgrade, enhancement, or other fee-based modification of your Cloud Service. In that event, we will provide a detailed quotation and scope of work prior to acting upon your Support Request.

Your cooperation, including information and materials reasonably required by us to provide such Support Services, will be necessary to permit us to address Support Requests that you submit.

Responding to Service Failures.

In the event of a Service Failure, you should immediately notify our general Customer Support mailbox (support@contractpodai.com) which is monitored 24/7/365. You should also notify your Customer Success Manager.

To assist us in resolving Service Failures, you must (a) provide all information and materials reasonably required to permit us to investigate, diagnose, address, and correct each Service Failure, and (b) make sure that all applications, data, interfaces, tools, software, hardware, and equipment within your control that are used in conjunction with the Cloud Service are properly maintained and functioning.

We will seek to meet any estimated completion times we provide (including the Target Resolution Times specified below) of any part of the Support Services.

Maintenance and Updates

We will use reasonable efforts to notify you in advance of any unscheduled maintenance and updates (including urgent or emergency maintenance). Scheduled maintenance and updates will take place at weekends and we will provide at least 5 days' notice of any scheduled maintenance or updates that may result in any downtime.

We host the Cloud Service and might update the content, functionality, and user interface of the Cloud Service from time to time.

Availability

We will provide access to the Cloud Service twenty-four hours a day, seven days per week (24x7) basis at a rate of at least 99.9%. Downtime due to maintenance and upgrades as set out above is excluded from any calculation of availability. If this availability is not achieved in any two consecutive months or three out of any six months you may terminate this Agreement with no penalty (and we will refund your pre-paid but unused fees), as your sole and exclusive remedy for our failure to meet availability or support commitments.

Service Levels

In the event of a Service Failure, we will acknowledge receipt as soon as possible. We will prioritize Service Failures in accordance with the priority matrix below:

PRIORITY MATRIX	
Critical/Crash (P1)	A crisis has occurred - the system is down or inaccessible or a major operational function (such as access to the document repository) becomes unavailable.
High Severity (P2)	Any problem imperative to continued success and requiring prompt resolution (e.g.: production system is functioning, but the capabilities become impaired (such as the ability to generate templates or a failure of an integration via API) or the system becomes unstable with periodic interruptions).
Medium Severity (P3)	These is a problem that occurs which needs to be resolved as quickly as possible but may have acceptable workarounds (e.g.: issues occur in production systems but the core system is still functional (for example issues with third party review functionality)
Low Impact (P4)	Situations that are technical questions or issues requiring a "how-to" or "how do I" answer (e.g.: clarification of procedures or information in documentation; attributes or options operating but not as expected; incorrect documentation). This also includes lower priority functional or visual changes requested by a customer.

The following table outlines the target time that we will work to resolve a Service Failure, based on its Priority Level:

Priority Code	Urgency of Response	Target Resolution Time
P1	Immediate, sustained effort using all necessary and available resources until service is restored	6 hours
P2	Prompt response to assess the situation, staff may be interrupted and taken away from lower priority jobs	48 hours (but will aim to resolve as quickly as possible)
P3	Response using standard procedures and operating within the normal frameworks	14 days
P4	Response using standard procedures and operating within the normal frameworks	Typically resolved with a new release or sub-release.

It is noted that to address an issue, a new code release may be necessary. For P1 and P2 issues, if a patch is required, we will address with a "hotfix" as soon as practical. For a P3 or a P4 issue we will generally address in our next scheduled release. Scheduled releases generally take place every 8 weeks.

Progress against Target Resolution Times will be measured from the time that all relevant information has been received from you to investigate the Service Failure.

Exclusions

We are not responsible for resolving Service Failures that result from any of the following:

Any modification, repair, or addition to the Cloud Service made by any person other than us (or any person authorized by us in writing);

Any fault or any issues in any equipment or in any third-party software used by you in conjunction with the Cloud Service;

Faults or unavailability caused by a Force Majeure Event or circumstances beyond our reasonable control; and

Your breach of the Acceptable Use Policy.

ANNEX B: ONEDPA DATA PROCESSING ADDENDUM

PARTIES AND EXECUTION	
Entity details: **Customer (as defined in the Main Agreement)**	Entity details: **Provider (as defined in the Main Agreement)**

VARIABLES		
Parties' relationship	Controller to Processor	
Parties' roles	Customer will act as the **Controller** (and for CCPA purposes, a Business) (as defined in Section 1 of the Terms) Provider will act as the **Processor** (and for CCPA purposes, a Service Provider) (as defined in Section 1 of the Terms)	
Contacts	**Controller**	**Processor**
	The individual and/or email specified in the Cover Page or the Order Form, as applicable.	Name: Bill Fitzgerald Email: privacy@contractpodai.com
Main Agreement	The *Bonterms Cloud Terms (Version 1.0)* to which this DPA is attached.	
Term	The Processing will continue until the expiration or termination of the Main Agreement.	
Breach Notification Period	Without undue delay after becoming aware of a personal data breach	
Sub-processor Notification Period	A reasonable timeframe before the new sub-processor is granted access to Personal Data	
Liability Cap	Each party's aggregate liability under this DPA will not exceed the liability caps as per the Main Agreement	
Governing Law and Jurisdiction	As per the Main Agreement	
Data Protection Laws	All laws, regulations and court orders which apply to the processing of Personal Data in: • the European Economic Area (**EEA**), • the United Kingdom (**UK**), • the United States of America (**US**),	

	• Australia, • Canada, • Japan This includes the European Union Regulation (EU) 2016/679, the Data Protection Act 2018, California Consumer Privacy Act of 2018 (**CCPA**)/California Privacy Rights Act of 2020 (**CPRA**), the Privacy Act 1998 and similar applicable laws, each as amended from time to time.
Services related to processing	Performance of the Cloud Services pursuant to the applicable Order Form and the Main Agreement.
Duration of processing	Processing will continue until the expiration or termination of the Main Agreement.
Nature and purpose of processing	Processor will process personal data as necessary to perform the Cloud Service pursuant to the Order Form, the Main Agreement, and as further instructed by the Controller in its use of the Cloud Service.
Personal Data	The types of personal data processed — the extent of which is determined and controlled by Controller in its sole discretion — may include: • First and last name • Title • Position • Employer • Contact information (company, email, phone, physical business address) • Identification Data (notably email addresses and phone numbers) • Electronic identification data (notably IP addresses and mobile device IDs)
Data subjects	The individuals whose personal data will be processed are fully determined by the Controller, and may include the following: • Prospects, customers, business partners and vendors of Customer (who are natural persons) • Employees or contact persons of Customer's prospects, customers, business partners and vendors • Employees, agents, advisors, freelancers of Customer (who are natural persons)
Special provisions	Sale of Customer Personal Data Prohibited. Processor shall not sell personal data as the term "sell" is defined by the CCPA/CPRA.

	CCPA/CPRA Certification. Processor hereby certifies that it understands its restrictions and obligations set forth in this DPA and will comply with them.
Transfer Mechanism	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 International Data Transfer Addendum issued by the Information Commissioner's Office under Section 119A of the Data Protection Act 2018, effective from 21 March 2022
ANNEX 1	
Security measures. Technical and organisational measures to ensure the security of Personal Data	Please visit https://contractpodai.com/resources/security-information-datasheet/ for the latest ContractPodAi security information datasheet.

ANNEX 2

Sub-processors. Current 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 EU
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
	Sendgrid	Email Send Service	USA
	ContractPod Solutions Pvt. Ltd.	Services & Support	Republic of India
	ContractPod Technologies Inc.	Services & Support	United States of America
	ContractPod Technologies Ltd.	Services & Support	United Kingdom Canada
	ContractPod Technologies (Asia Pacific) Pty. Ltd.	Services & Support	Australia

TERMS

1. What is this agreement about?

1.1 **Purpose**. The parties are entering into this Data Processing Agreement (**DPA**) for the purpose of processing Personal Data (as defined above).

1.2 **Definitions.** Under this DPA:

(a) **adequate country** means a country or territory that is recognised under Data Protection Laws from time to time as providing adequate protection for processing Personal Data**,**

(b) **Controller**, **data subject**, **personal data breach**, **process/processing**, **Processor**, and **supervisory authority** have the same meanings as in the Data Protection Laws,

(c) **Business** and **Service Provider** have the same meanings as in the CCPA/CPRA, and

(d) **Sub-processor** means another processor engaged by the Processor to carry out specific processing activities with Personal Data.

2. What are each party's obligations?

2.1 **Controller obligations**. Controller instructs Processor to process Personal Data in accordance with this DPA, and is responsible for providing all notices and obtaining all consents, licences and legal bases required to allow Processor to process Personal Data.

2.2 **Processor obligations.** Processor will:

(a) only process Personal Data in accordance with this DPA and Controller's instructions (unless legally required to do otherwise),

(b) not sell, retain or use any Personal Data for any purpose other than as permitted by this DPA and the Main Agreement,

(c) inform Controller immediately if (in its opinion) any instructions infringe Data Protection Laws,

(d) use the appropriate technical and organisational measures described in Annex 1 when processing Personal Data to ensure a level of security appropriate to the risk involved,

(e) notify Controller of a personal data breach within the Breach Notification Period and provide assistance to Controller as required under Data Protection Laws in responding to it,

(f) ensure that anyone authorised to process Personal Data is committed to confidentiality obligations,

(g) without undue delay, provide Controller with reasonable assistance with:

(i) data protection impact assessments,

(ii) responses to data subjects' requests to exercise their rights under Data Protection Laws, and

(iii) engagement with supervisory authorities,

(h) if requested, provide Controller with information necessary to demonstrate its compliance with obligations under Data Protection Laws and this DPA,

(i) allow for audits at Controller's reasonable request, provided that audits are limited to once a year and during business hours except in the event of a personal data breach, and

(j) return Personal Data upon Controller's written request or delete Personal Data by the end of the Term, unless retention is legally required.

2.3 **Warranties.** The parties warrant that they and any staff and/or subcontractors will comply with their respective obligations under Data Protection Laws for the Term.

3. Sub-processing

3.1 **Use of sub-processors.** Controller authorises Processor engage other processors (referred to in this section as **sub-processors**) when processing Personal Data. Processor's existing sub-processors are listed in Annex 2.

3.2 **Sub-processor requirements.** Processor will:

(a) require its sub-processors to comply with equivalent terms as Processor's obligations in this DPA,

(b) ensure appropriate safeguards are in place before internationally transferring personal data to its sub-processor, and

(c) be liable for any acts, errors or omissions of its sub-processors as if they were a party to this DPA.

3.3 **Approvals.** Processor may appoint new sub-processors provided that they notify Controller in writing in accordance with the Sub-processor Notification Period.

3.4 **Objections.** Controller may reasonably object in writing to any future sub-processor. If the parties cannot agree on a solution within a reasonable time, either party may terminate this DPA.

4. International personal data transfers

4.1 **Instructions.** Processor will transfer Personal Data outside the UK, the EEA or an adequate country only on documented instructions from Controller, unless otherwise required by law.

4.2 **Transfer mechanism.** Where a party is located outside the UK, the EEA or an adequate country and receives Personal Data:

(a) that party will act as the data importer,

(b) the other party is the data exporter, and

(c) the relevant Transfer Mechanism will apply.

4.3 **Additional Measures.** If the Transfer Mechanism is insufficient to safeguard the transferred Personal Data, the data importer will promptly implement supplementary measures to ensure Personal Data is protected to the same standard as required under Data Protection Laws.

4.4 **Disclosures.** Subject to terms of the relevant Transfer Mechanism, if the data importer receives a request from a public authority to access Personal Data, it will (if legally allowed):

(a) challenge the request and promptly notify the data exporter about it, and

(b) only disclose to the public authority the minimum amount of Personal Data required and keep a record of the disclosure.

5. Other important information

5.1 **Survival**. Any provision of this DPA which is intended to survive the Term will remain in full force.

5.2 **Order of precedence.** In case of a conflict between this DPA and other relevant agreements, they will take priority in this order:

(a) Transfer Mechanism,

(b) DPA,

(c) Main Agreement.

5.3 **Notices**. Formal notices under this DPA must be in writing and sent to the Contact on the DPA's front page as may be updated by a party to the other in writing.

5.4 **Third parties.** Except for affiliates, no one other than a party to this DPA has the right to enforce any of its terms.

5.5 **Entire agreement.** This DPA supersedes all prior discussions and agreements and constitutes the entire agreement between the parties with respect to its subject matter and neither party has relied on any statement or representation of any person in entering into this DPA.

5.6 **Amendments.** Any amendments to this DPA must be agreed in writing.

5.7 **Assignment.** Neither party can assign this DPA to anyone else without the other party's consent.

5.8 **Waiver.** If a party fails to enforce a right under this DPA, that is not a waiver of that right at any time.

5.9 **Governing law and jurisdiction.** The Governing Law applies to this DPA and all disputes will only be litigated in the courts of the Jurisdiction.

EEA STANDARD CONTRACTUAL CLAUSES

MODULE 2 (C2P) AND ANNEXES

SCHEDULE TO THE DATA PROCESSING AGREEMENT

PARTIES AND EXECUTION	
Purpose. This Schedule supplements the Data Processing Agreement entered into between the parties (the **DPA**) to govern the international transfer of personal data. By signing below, the parties agree to the terms of this Schedule.	
Data exporter	**Data importer**
Entity details: **CONTROLLER (Customer)**	Entity details: **PROCESSOR (Provider)**

VARIABLES	
Docking	Clause 7 of the Clauses does not apply.
Use of sub-processors	No changes are made to Clause 9 in the Clauses.
Redress	No changes are made to Clause 11 in the Clauses
Supervision	Clause 13(a) is deleted in its entirety and replaced with the following: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.
Governing law	No changes are made to Clause 17 in the Clauses

ANNEX I

A. LIST OF PARTIES	
Data exporter	
Name	As described in the Parties and Execution table at the beginning of this Schedule
Address	As described in the Parties and Execution table at the beginning of this Schedule
Contact person's name, position and contact details	As described in the Parties and Execution table at the beginning of this Schedule

Activities relevant to the data transferred under these Clauses	As described in the Variables table at the beginning of the DPA
Signature and date	
Role	CONTROLLER
Data importer	
Name	As described in the Parties and Execution table at the beginning of this Schedule
Address	As described in the Parties and Execution table at the beginning of this Schedule
Contact person's name, position and contact details	As described in the Parties and Execution table at the beginning of this Schedule
Activities relevant to the data transferred under these Clauses	As described in the Variables table at the beginning of the DPA
Signature and date	
Role	PROCESSOR

B. DESCRIPTION OF TRANSFER	
Term	***Description***
Data subjects. Categories of data subjects whose personal data is transferred	As described in the Variables table in the DPA
Personal data. Categories of personal data transferred	As described in the Variables table in the DPA
Sensitive data. Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data,	As described in the Variables table in the DPA

restrictions for onward transfers or additional security measures	
Transfer frequency. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)	As described in the Variables table in the DPA
Nature of the processing	As described in the Variables table in the DPA
Purpose of the data transfer and further processing	As described in the Variables table in the DPA
Retention period. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	Within ninety (90) calendar days of the Main Agreement's expiration or termination, Processor will securely destroy (in accordance with standard industry practices for deletion of personal data) all copies of Controller's personal data. 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. Tapes, printed output, optical disks, and other physical media will be physically destroyed by a secure method and by a recognized provider. Upon Controller's request, Processor will provide a Certificate of Destruction that Processor has deleted all Controller's personal data. Processor will provide the "Certificate of Deletion" within thirty (30) calendar days of Controller's request.
Sub-processor transfers. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	As described in Annex 2 of the DPA

C. COMPETENT SUPERVISORY AUTHORITY	
Supervisory authority. Identify the competent supervisory authority/ies in accordance with Clause 13	The Republic of Ireland

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES	
Measures. Technical and organisational measures to ensure the security of the data	As described in Annex 1 of the DPA

ANNEX III

LIST OF SUB-PROCESSORS	
Sub-processors. The controller has authorised the use of sub-processors	As described in Annex 2 of the DPA

UNITED KINGDOM
INTERNATIONAL DATA TRANSFER ADDENDUM SCHEDULE

Purpose. This Schedule supplements the Data Processing Agreement entered into between the parties (the **DPA**) to govern the international transfer of personal data. By signing below, the parties agree to the terms of this Schedule.

PART 1: TABLES

TABLE 1		
Start date	As per the Main Agreement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**

TABLE 2	
Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information

TABLE 3	
Appendix Information means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:	
Annex 1A	List of Parties: As described in the Module 2 Schedule to the DPA
Annex 1B	Description of Transfer: As described in the Module 2 Schedule to the DPA
Annex II	Technical and organisational measures including technical and organisational measures to ensure the security of the data: As described in Annex II of the DPA
Annex III	List of Sub-processors: As described in Annex I of the DPA

TABLE 4	
Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: Neither Party.

PART 2: MANDATORY CLAUSES

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

ANNEX C: ACCEPTABLE USE POLICY FOR CONTRACTPODAI CLOUD SERVICES

You and your Users will not use the Cloud Service in any way that violates the terms of this **Acceptable Use Policy ("AUP")** or for any purpose or in any manner that is unlawful or prohibited by the ContractPodAi Master Terms and Annexes.

You will comply (and your Users will comply) with our AUP, as follows:

Prohibited Activities. You will not and will ensure that your Users will not:

1. copy, reproduce, publish, distribute, redistribute, transmit, modify, adapt, sublicense, sell, transfer, assign, rent, disclose (whether or not for charge), or in any way commercially exploit the Cloud Service;
2. permit use of the Cloud Service in any manner by a third-party (except as otherwise permitted in the Master Terms and Annexes;
3. use the Cloud Service to: (a) send unsolicited or unlawful messages; (b) send or store infringing, obscene, threatening, harmful, libelous, or otherwise unlawful material, including material harmful to children or to violate privacy rights (*however, this will not prohibit you from sending or storing such material if such material is related to a lawful purpose and is being used in the course of legal work*); (c) send or store material containing software viruses, worms, Trojan horses or other harmful computer code, files, scripts, or agents; (d) interfere with or disrupt the integrity or performance of the Cloud Service or the data contained therein; (e) attempt to gain unauthorized access to the Cloud Service or related systems or networks; or (f) provide or disclose to, or permit use of the Cloud Service by, persons other than Users;
4. make alterations to, or modifications of, the whole or any part of the Cloud Service nor permit the Cloud Service or any part of it to be combined with, or become incorporated in, or merged with any other programs; and
5. disassemble, decompile, reverse engineer, or create derivative works based on the whole or any part of the Cloud Service nor attempt to do any such things except to the extent that such actions cannot be prohibited because they are essential for the purpose of achieving inter-operability of the Cloud Service with another software program, and provided that the information obtained by you during such activities: (a) is used only for the purpose of achieving inter-operability of the Cloud Service with another software program; (b) is not disclosed or communicated without our prior written consent to any third party; and (c) is not used to create any software which is substantially similar to the Cloud Service.

Violations of the AUP. We may immediately suspend your access to the Cloud Service if you breach the AUP or do not respond to us in a reasonable period after we have contacted you about a potential breach of the AUP. We may also suspend your access the Cloud Service and/or we may terminate your Order(s) and this Agreement for cause. We are not obligated to (but may choose to) remove any prohibited materials and deny access to any person or entity that violates the AUP. We further reserve all other rights.