LEAH

The Explainer: Why Leah Uses Bonterms Cloud Terms and DPA

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

Why Bonterms? Bonterms are designed to be **a neutral starting point** for an agreement that meets the needs of both Leah 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. 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)!

Data processing agreements are long, extensive, and an unfortunate necessity in the world today. The **Bonterms DPA** 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 Leah to move through understanding how we protect your trusted data and information.

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

- **Best-practice?** Bonterms documents were drafted and extensively reviewed and revised by a 100+ 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 DPA was worked up by lawyers and data privacy professionals across the globe to create a standard DPA that can be used nearly anywhere on Earth.
- **Balanced?** Both Bonterms DPA and 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 Bonterms DPA are free to use under CC BY 4.0.

The entire Leah 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.

Contents

LEAH

Main Agreement: Bonterms Cloud Terms (V. 1.0)[1]

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.

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

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

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 use the Cloud Service for High Risk Activities, 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.

(a) 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.

(b) 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.

(c) 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.

(a) 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.

(b) 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.

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.

Attachment A: 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 Attachment 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 (categorized as P1, P2 or P3 as per the priority matrix below).
- **"Support Desk"** means our helpdesk to be contacted in the event of a Service Failure which is available 24/7/365.
- **"Support Plan"** means our Standard, Gold or Platinum plans. Your Plan is set out in the Order Form.
- **"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.
- **"Working Hours"** means 8am – 6pm on business days in the territory of your head office as set out in the Order Form.

Note: Working Hours are only applicable to Standard Support Plan customers; for Gold and Platinum Support Plan Customers, Support Desk operation and Target Resolution Times are based on 24/7/365.

Scope of Support Services

Support Requests

You will have a designated Customer Success Manager whose contact information will be shared with you.

Support Requests should be sent to our general Customer Support mailbox (*support@leahai.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, configuration change, 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.

Examples of Support Requests include issues that are technical questions or issues requiring a "how-to" or "how do I" answer (e.g.: clarification of procedures or information in documentation; assistance with understanding or modifying system attributes or options; correcting issues with documentation or training materials; or issues with data migration). This also includes lower priority functional or visual changes.

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.

Service Failures

In the event of a Service Failure, you should immediately contact us via the Support Desk Portal, details of which will be supplied to you. The Support Desk Portal is monitored 24/7/365 for Gold and Platinum Support Customers and during Working House for Standard Support Customers. In addition, Platinum Support Plan customers will also be supplied with telephone contact details of the Support Desk.
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. For Standard Support Plan Customers, the Support Desk will only respond during Working Hours.

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.

Uptime Availability

The Cloud Service will be up and available twenty-four hours a day, seven days per week (24x7) basis at a rate of at least the amount set out below, depending on your Support Plan ("Uptime Availability").

Standard: 99.00%	Gold: 99.5%	Platinum: 99.9%

Downtime due to scheduled maintenance and upgrades as set out above is excluded from any calculation of availability. If the Uptime Availability is not achieved in any three consecutive months or four out of any six consecutive 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 commitments.

Service Failure Priorities

We prioritize Service Failures in accordance with the priority matrix below:

Critical/Crash (P1)	A crisis has occurred - a major operational function becomes unusable (such as the document repository being completely inaccessible after login). If the Cloud Service is completely unavailable and cannot be reached, this will be calculated as part of our Uptime Availability and not as a Service Failure.
High Severity (P2)	Any problem imperative to continued success and requiring prompt resolution (e.g.: production system is functioning, but the capabilities become seriously 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 workarounds are available (for example: email send fails when creating an invitation email for the third-party review functionality, but an invite link may still be generated and sent by the user).
Configuration Issues and Changes	Configuration issues or requests to change the configuration of the Cloud Service will not be considered Service Failures unless we have materially failed to comply with the implementation SOW or a change order.

The following table outlines the urgency of response that we will apply to resolve a Service Failure, based on its Priority Level:

Priority	Urgency of Response	Target Resolution Time		
		Standard	Gold	Platinum
P1	Using all necessary and available resources until functionality is restored	2 Working Days	1 Working Day	8 Hours
P2	Prompt response to assess the situation, staff may be reassigned from lower priority jobs	5 Working Days	3 Calendar Days	2 Calendar Days
P3	Response using standard procedures and operating within the normal frameworks	30 Calendar Days	14 Calendar Days	7 Calendar Days

Kindly note 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 issue we will generally address in our next scheduled release. Scheduled releases generally take place every 12 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 authorized by us.
- Any fault or error in any equipment or in any third-party software used by you in conjunction with the Cloud Service (except for a fault in an API or connector supplied by us, in which case such fault will be treated as a Service Failure). Where a fault occurs with third-party

software and/or equipment integrated with or connected to the Cloud Service, we will provide reasonable technical assistance regarding the Cloud Service to enable you to reconnect or re-integrate such third-party software or equipment.

- Faults or unavailability caused by a Force Majeure Event or circumstances beyond our reasonable control.

General Support Terms for API-only Integrations

The following terms apply to all API-only Integrations:

- Provider will supply comprehensive API documentation and Swagger specifications (technical descriptions of each API endpoint); Customer should thoroughly review these materials before requesting technical assistance.
- API support via videoconference or teleconference becomes available only after Customer has attempted implementation using the provided documentation. Customer must demonstrate specific issues or errors encountered during their implementation attempts.
- Customer must provide a clear description of their integration objectives in order to help Provider's support team understand the context and provide relevant assistance.
- API support addresses specific questions about API structure, payloads, and responses as they exist. Support team cannot provide custom integration development or implementation of Customer's specific use cases; assistance is limited to explaining how to use the existing APIs as designed.
- Provider's development team cannot access Customer's production systems or credentials and demonstrations and troubleshooting will use test environments (QA/UAT) only.
- Support for API-only Integrations are limited to a maximum of 10 hours unless otherwise agreed or specified.

Attachment 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				
Agreement	This DPA is an Attachment to the Order Form and Agreement between «Client_Name» ("Customer") and Leah ("Provider")[2], with Leah Request ID: #«Request_ID».			
DPA Effective Date	Effective the date of the referenced Order Form and Agreement between Customer and Provider.			
Subprocessor List[3]	**Sub-Processor**	**Purpose**	**Location[4]**	**Products Used In**
	ABBY OCR SDK	Converting pdf and scanned document in a format acceptable to IBM Watson for AI processing	EU	CLM (only for customers who went live pre-2021)
	Anthropic	Leah Functionality (no Customer Data is stored or retained by Anthropic)	USA Japan EU / UK	Leah
	Codestone Solutions Ltd.	Customer Success & Support (Team Dedicated to Provider)	UK / EU	All (Support Routing and First-Level Support Services)
	Cohere	Leah Functionality (no Customer Data is stored or retained by Cohere)	Canada USA EU / UK Japan	Leah
	ContractPod Solutions Pvt. Ltd.	Services & Support	Republic of India	All (When Necessary)
	ContractPod Technologies (Asia Pacific) Pty. Ltd.	Services & Support	Australia	All (When Necessary)
	ContractPod Technologies Inc.	Services & Support	United States of America	All (When Necessary)

[2] «Legal_Party_Name» trading as / dba Leah.
[3] Not all subprocessors will be applicable to all Leah customers. For example, depending on your eSignature solution, either DocuSign or AdobeSign will be used, to the exclusion of the other.
[4] Sub-Processors with multiple locations are selected based on Customer's hosting region (such as an EU or adequate country sub-processor for EU PII).

ContractPod Technologies Ltd.	Services & Support	United Kingdom Canada	All (When Necessary)
DocuSign or **Adobe**	Electronic signature	EU USA	CLM
Freshworks Inc.	Helpdesk/ticketing system for customer support management	Per selected data hosting region; see freshworks.com/privacy/data-hosting	All (Used for Customer Support and Success Ticketing)
Google AI/ML; Google Cloud	Leah Functionality (no Customer Data is stored or retained by Google); Data hosting for Google Cloud Customers	USA Japan EU / CH / UK	Leah
Jitterbit	API connectivity for non-standard integrations.	EU US	CLM
Microsoft Azure Services	Data Hosting, Translation, Microsoft Office Services (if using WOPI services)	EU USA Australia	CLM Leah
Oracle Cloud	Data Hosting	EU/UK/CH USA Australia India	CLM Leah
OpenAI LLC	Leah Functionality (no Customer Data is stored or retained by OpenAI)	USA Japan EU / CH	Leah
QlikTech International AB	Reporting and Graphing for DeepSights	Ireland, Frankfurt, London (UK/EU/CH) USA Australia, Singapore (APAC)	CLM
Sendgrid	Email Send Service	USA	CLM
Totango Inc.	Customer Success & Support Tracking – No client access.	US / EU	All (Used for Customer Success Management Recordkeeping)
ZOHO Corporation Pvt. Ltd.	Document collaboration (if using ZOHO services)	EU	CLM
Zuva Inc.	Document Intelligence	USA Japan EU	CLM

Schedules *(attach)*	
The following Schedules are incorporated into this DPA:	
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	

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

Name:	**Customer, as specified in the Order Form.**
Contact details for data protection:	The individual and/or email specified in the Cover Page or the Order Form, as applicable.
Main address:	The Customer's address specified in the Cover Page or the Order Form, as applicable.
Role:	Controller

Provider / 'Data Importer' Details

Name:	**Provider, as specified in the Order Form.**
Contact details for data protection:	Name: Leah Privacy & Security Team Email: privacy@leahai.com
Main address:	The Provider's address, as specified in the Cover Page or the Order Form, as applicable.
Provider activities:	Provider offers legal technology services including contract lifecycle management, document storage, document analysis, and other technologies for support of Customer's activities.
Role:	Processor

Details of Processing

Categories of 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)
Categories of Customer 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)
Sensitive Categories of Data	NONE.
Frequency of transfer:	The Processing will continue until the expiration or termination of the Main Agreement.
Nature of the Processing:	Processor will process personal data as necessary to perform the Cloud Service pursuant to the Order Form, the Agreement, and as further instructed by the Controller in its use of the Cloud Service.

Purpose of the Processing:	Performance of the Cloud Services pursuant to the applicable Order Form and the Main Agreement.
Duration of Processing / retention period:	• Processing will continue until the expiration or termination of the Agreement. • 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. • 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.
Transfers to Subprocessors:	• 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 United Kingdom's Information Commissioner's Office under Section 119A of the Data Protection Act 2018, effective from 21 March 2022.

Schedule 2: Technical and Organizational Measures

Please visit https://www.leahai.com/trust-portal/ 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:

"**Designated EU Governing Law**" means:	Republic of Ireland
"**Designated EU Member State**" means:	Republic of Ireland

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.

Attachment C: Acceptable Use Policy & Fair Use Policy

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

1. **Prohibited Activities.** You will not and will ensure that your Users will not:
   - 1.1. 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;
   - 1.2. permit use of the Cloud Service in any manner by a third-party (except as otherwise permitted in the Agreement;
   - 1.3. use the Cloud Service to:
     - 1.3.1. send unsolicited or unlawful messages;
     - 1.3.2. 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);
     - 1.3.3. send or store material containing software viruses, worms, Trojan horses or other harmful computer code, files, scripts, or agents;
     - 1.3.4. interfere with or disrupt the integrity or performance of the Cloud Service or the data contained therein;
     - 1.3.5. attempt to gain unauthorized access to the Cloud Service or related systems or networks; or
     - 1.3.6. provide or disclose to, or permit use of the Cloud Service by, persons other than Users;
   - 1.4. 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
   - 1.5. 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:
     - 1.5.1. is used only for the purpose of achieving inter-operability of the Cloud Service with another software program;
     - 1.5.2. is not disclosed or communicated without our prior written consent to any third party; and
     - 1.5.3. is not used to create any software which is substantially similar to the Cloud Service.
2. **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.
3. **Fair Use Policy.** Provider offers unlimited access to the Cloud Service subject to this Fair Use Policy. Provider reserves the right, in its sole discretion, to monitor, throttle, rate-limit, or otherwise restrict Customer's access to the Cloud Service at any time if Provider determines that Customer's consumption of computational resources — including CPU / "compute," memory, API calls, data storage, or data transfer — is excessive, disproportionate, or otherwise inconsistent with normal usage patterns for subscribers on an equivalent tier. Provider will use reasonable efforts to notify Customer prior to taking any such action, except where Provider determines that immediate action is necessary to protect the performance, stability, or security of the Platform. Nothing in this Fair Use Policy limits Provider's right to offer Customer an upgraded capacity tier or other options as a remedy for excessive use.

Attachment D: AI Terms

The following terms ("**AI Terms**") are hereby added to and become part of the Agreement as Additional Terms. Capitalized terms not defined in these AI Terms have the meanings given in the Agreement. The Agreement applies to the AI Features as part of the Cloud Service with the following modifications.

1. **Use of AI Features**. Customer may submit Customer Data (including in the form of prompts or queries) to the AI Features ("**Inputs**") and receive outputs from the AI Features ("**Outputs**"). "**AI Features**" means the features included in Leah (whether Standalone or

integrated with the CLM), including large language models (LLMs) or other machine learning or artificial intelligence features of the Product(s).

2. **Training**: Provider may not use Inputs or Outputs to train or otherwise improve AI Features, except solely for the benefit of Customer.
3. **Intellectual Property**: Inputs and Outputs are deemed to be Customer Data, subject to these AI Terms.
4. **Similar Output**. Customer acknowledges that Outputs provided to Customer may be similar or identical to Outputs independently provided by Provider to others.
5. **Infringement by Output**. Due to the nature of the AI Features, Provider does not represent or warrant that (a) Output does not incorporate or reflect third-party content or materials or (b) Output will not infringe third-party intellectual property rights. Claims of intellectual property infringement or misappropriation by Output are not included in Provider-Covered Claims.
6. **Disclaimer**. Outputs are generated through machine learning processes and are not tested, verified, endorsed or guaranteed to be accurate, complete or current by Provider. Customer should independently review and verify all Outputs as to appropriateness for any or all Customer use cases or applications. The warranty disclaimers and limitations of liability in the Agreement for the Product(s) apply to the AI Features.
7. **Third-party Providers**. Provider has specified in Provider's DPA any third parties that provide the AI Features.
8. **Special Restrictions on Use of AI Features**. The following restrictions are deemed part of the AUP under Section 9.1 (Compliance) of the Standard Agreement. Without limiting any restrictions on use of the Product(s) in the Standard Agreement, Customer will not and will not permit anyone else to (a) use the AI Features or any Output to infringe any third-party rights, (b) use the AI Features or any Output to develop, train or improve any AI or ML models (separate from authorized use of the Product(s) under this Agreement), (c) represent any Output as being approved or vetted by Provider, (d) represent any Output as being an original work or a wholly human-generated work, (e) use the AI Features for automated decision-making that has legal or similarly significant effects on individuals, unless it does so with adequate and qualified human review and in compliance with Laws, or (f) use the AI Features for purposes or with effects that are discriminatory, harassing, harmful or unethical.

Attachment E: EU Data Act Terms (Only Where Applicable)

1. **EU Data Act Switching Rights.** Customers subject to EU Regulation EU2023/2854 ("Data Act") have the statutory right to terminate their Order Form for Cloud Services at any time, regardless of the initial Subscription Term or any renewal period. Customer will provide 60 days' written notice to Provider ("Switching Notice Period"). Upon notice, Customer may (a) switch to a different data processing services provider, (b) switch to Customer's on-premises data processing solution, or (c) erase Customer Data from the Cloud Service without switching.

2. **Switching Timeline.**
   a. Base Period. Provider will continue Cloud Services throughout the 60-day Switching Notice Period. The Order Form remains in effect under the same terms. Customer will pay all Subscription Fees during this period.
   b. Transitional Period. Customer has 30 days after the Switching Notice Period ends to complete data transfer (the "Transitional Period"). The Order Form remains in effect. Customer will pay all applicable fees.

3. **Provider Obligations During Switching.** Provider will (a) continue Cloud Services throughout the Switching Notice Period and Transitional Period, (b) provide Customer Data in XML, XLSX, CSV, or similar industry standard formats, (c) maintain data availability for up to 60 days after the Transitional Period ends, (d) provide reasonable technical assistance to facilitate switching, and (e) delete all Customer Data after the 60-day post-transition period or upon Customer instruction. After January 12, 2027, Provider will provide all standard switching services in this Clause 3 at no additional charge (beyond applicable Subscription Fees). Requests that fall outside the scope of this Clause 3 are not mandated by the Data Act and may be charged at Provider's standard rates.

4. **Customer Obligations During Switching.**
   a. Data Migration. Customer will (i) perform all data migration to new providers or on-premises systems at its own risk, (ii) take all reasonable measures to achieve effective switching, (iii) perform all import and implementation of Customer Data into new systems, and (iv) act in good faith to implement Provider's switching process instructions. Customer may use third parties for migration tasks.
   b. End of Cloud Service Access. All Customer rights to the Cloud Service end when the Transitional Period expires. Customer will stop using the Cloud Service at that time.
   c. Intellectual Property Protection. Customer and any third parties involved in switching must comply with the confidentiality and intellectual property obligations in the Agreement. Customer may share Provider materials with third parties only to the minimum extent necessary to complete the migration, and only subject to confidentiality obligations no less protective than those in the Agreement.
   d. Loss of Switching Rights. Customer loses Transitional Period rights if (i) Customer has unpaid Subscription Fees for the terminated Cloud Services, or (ii) applying the Data Act would require Provider to violate applicable legal requirements.

5. **Early Termination Fee.**
   a. Amount. Customer will pay an early termination fee ("ETF") equal to all remaining Subscription Fees through the current Subscription Term expiration date. Provider will credit any prepaid amounts toward the ETF. Prepaid Subscription Fees are non-refundable. The ETF is due within 30 days of the Switching Notice Period beginning.
   b. Legal Basis. This ETF constitutes an early termination charge under Article 29(4) of the Data Act, not a switching charge. The ETF reflects Provider's legitimate business interest in recovering costs associated with providing fixed-term pricing and service commitments.

c. Effect on Payment Obligations. Switching does not relieve Customer of the obligation to pay any Subscription Fees or ETF accrued or payable to Provider.

6. **Pre-Contractual Disclosure and Acknowledgement.** Customer acknowledges receiving clear information about standard fees and early termination charges before executing the Order Form, as required by Article 29 of the Data Act.