DOCUMENT RECORD

VERSION	EFFECTIVE	GOVERNING TEXT
2026-09-17	September 17, 2026	English

REFERENCE
legal.dapta.ai/en/documents/nda/versions/2026-09-17

Mutual Confidentiality and Data Protection Agreement

This Mutual Confidentiality and Data Protection Agreement (the “Agreement”) is entered into by and between Dapta, Inc., a Delaware corporation (“Dapta”), and the company identified in the signature block below (“Customer”). Dapta and Customer are each a “Party” and together the “Parties.”

The Parties are evaluating, negotiating, or carrying out a business relationship under which Dapta may provide its software platform and related services to Customer (the “Purpose”). This Agreement is effective on the date Customer signs it (the “Effective Date”). Dapta accepts this Agreement by offering it for online signature.

1. Confidential Information

“Confidential Information” means non-public information that a Party or its Affiliates (“Discloser”) discloses or makes available to the other Party (“Recipient”) in connection with the Purpose, in any form, that is identified as confidential or that a reasonable person would understand to be confidential given its nature and the circumstances of disclosure. Confidential Information includes information disclosed before, on, or after the Effective Date in connection with the Purpose, and any notes, analyses, and derived data, such as embeddings, indexes, and logs, that contain or reasonably reveal it.

Customer’s Confidential Information includes its non-public business, technical, financial, operational, employee, customer, and product information; credentials and access keys; integration details; and data, content, prompts, instructions, files, and other materials that Customer or its users submit to, load into, or share through Dapta’s services (“Customer Data”). Customer Data also includes Personal Data processed by Dapta on Customer’s behalf.

Dapta’s Confidential Information includes its non-public product, pricing, roadmap, architecture, source code, model and agent configurations, system prompts, documentation, security and compliance materials (such as audit reports, penetration test summaries, and completed security questionnaires), and other non-public information concerning Dapta’s technology or business. The existence and content of the Parties’ discussions are Confidential Information of both Parties.

“Affiliate” means an entity that controls, is controlled by, or is under common control with a Party. “Control” means ownership of more than fifty percent of the voting interests or equivalent authority.

Confidential Information does not include information that Recipient can demonstrate by contemporaneous written records: (a) is or becomes public through no breach of this Agreement; (b) was lawfully known to Recipient without a confidentiality obligation before disclosure; (c) was independently developed by Recipient without use of or reference to

Discloser's Confidential Information; or (d) was lawfully received from a third party without a confidentiality obligation.

These exclusions do not permit Recipient to disregard applicable data-protection, privacy, security, or professional-confidentiality obligations concerning Personal Data. Information is not excluded merely because individual elements are public if the combination, compilation, or context is not public.

2. Permitted Use and Protection

Recipient will use Discloser's Confidential Information solely to evaluate, negotiate, or perform the Purpose and will not use it for its own independent commercial benefit or for the benefit of any third party, except as expressly permitted by this Agreement or another written agreement between the Parties.

Recipient will protect Discloser's Confidential Information using at least the same degree of care it uses for its own information of similar sensitivity and, in all cases, no less than reasonable administrative, technical, and physical safeguards. Recipient will not remove proprietary or confidentiality markings; reverse engineer, decompile, or attempt to derive source code, models, model weights, system prompts, or other underlying components from Discloser's Confidential Information; or handle Confidential Information in violation of applicable export-control laws.

Nothing in this Agreement grants Recipient any ownership interest, license, or other right in Discloser's Confidential Information except the limited right to use it as expressly permitted here.

3. Representatives and Subprocessors

Recipient may disclose Discloser's Confidential Information to its and its Affiliates' employees, officers, contractors, auditors, and legal or financial advisers (collectively, "Representatives") who have a need to know the information for the Purpose and are bound by written confidentiality obligations at least as protective as this Agreement or, in the case of professional advisers, professional duties of confidentiality. Recipient remains responsible for its Representatives' compliance with this Agreement. Either Party may also disclose the existence and terms of this Agreement to its actual or prospective investors, lenders, and acquirers who are bound by confidentiality obligations.

For purposes of providing, securing, supporting, and maintaining the Dapta services, Dapta may disclose Customer Confidential Information, including Customer Data, to its subprocessors that need the information for those purposes. Dapta's current list of subprocessors and service providers is available at **https://trust.dapta.ai/en#subprocessors** (the "Subprocessor List"). The Subprocessor List is incorporated by reference only for identifying current subprocessors and may be updated under this Section. A provider may process Customer Data only after it has been identified on the Subprocessor List or otherwise approved in writing by Customer.

Dapta will:

(a) impose written confidentiality, privacy, and security obligations on each subprocessor that are no less protective of Customer Data than the obligations applicable to Dapta under this Agreement and any applicable data-processing addendum;

(b) remain responsible for each subprocessor's acts and omissions relating to Customer Data as if they were Dapta's own acts and omissions;

(c) maintain the Subprocessor List accurately;

(d) provide, upon reasonable request, the subprocessor's name, processing location, service description, and applicable security or privacy documentation; and

(e) require subprocessors to delete or return Customer Data when Dapta's deletion obligations under this Agreement or the applicable services agreement require deletion.

4. Customer Data and Personal Data

"Personal Data" means information relating to an identified or identifiable individual, or any equivalent term under Applicable Data Protection Law. "Applicable Data Protection Law" means the privacy, data-protection, and security laws applicable to the processing of Personal Data under the Purpose. "Applicable Law" means the laws, regulations, and governmental orders that apply to a Party or to the information concerned, including Applicable Data Protection Law.

Where Dapta processes Personal Data on Customer's behalf, the Parties will enter into an applicable data-processing addendum ("DPA"). The DPA governs the details of that processing and supplements this Agreement; if there is a conflict concerning Personal Data, the DPA controls, and this Agreement controls all other Confidential Information.

Dapta may process Customer Data only as necessary to provide, secure, support, maintain, and improve the services, as directed by Customer or as otherwise permitted by the applicable services agreement. Dapta will not sell Customer Data, use Customer Data for targeted advertising, or use Customer Data to train or fine-tune a general-purpose artificial-intelligence model, nor permit a subprocessor to do so, unless Customer expressly authorizes that use in writing.

Dapta may create and use aggregated and de-identified information derived from use of the services only if the information does not identify Customer, its users, or any individual, cannot reasonably be used to re-identify them, and does not reveal Customer-specific confidential information. Dapta will not attempt to re-identify such information or combine it with other information for that purpose. Dapta may use that information for service analytics, security, benchmarking, and improvement, provided that it does not disclose Customer's identity or confidential business information.

5. Artificial Intelligence

Recipient may process Discloser's Confidential Information with artificial-intelligence or machine-learning tools or services ("AI Tools") only in connection with the Purpose, and only if the provider of the AI Tool is bound by written confidentiality obligations at least as protective as this Agreement and is prohibited from using Discloser's Confidential Information, including inputs, prompts, files, and outputs, to train or improve models made available to anyone else, and from retaining it longer than needed to provide the AI Tool, including limited retention for security and abuse monitoring. When a subprocessor of Dapta provides an AI Tool, Section 3 also applies.

Except as Section 4 permits for Customer Data, Recipient will not use Discloser's Confidential Information to train, fine-tune, or otherwise improve any artificial-intelligence or machine-learning model, other than a model used solely to carry out the Purpose for Discloser, unless Discloser expressly authorizes that use in writing.

Outputs generated from Discloser's Confidential Information are Confidential Information of Discloser to the extent they contain or reasonably reveal it. This Agreement does not grant any right to use Discloser's Confidential Information retained in the memory of Recipient's Representatives or in any AI Tool, model, or dataset.

6. Feedback

If Customer voluntarily provides suggestions, enhancement requests, or other feedback about Dapta's services ("Feedback"), Dapta may use that Feedback to develop, improve, and operate its services without payment or obligation to Customer, provided that Dapta does not disclose Customer's Confidential Information or identify Customer as the

source of the Feedback without Customer's consent. Feedback does not include Customer Data, Personal Data, or Customer's confidential business information.

7. Security Incident

Recipient will notify Discloser without undue delay, and in no event later than seventy-two hours after becoming aware, of any unauthorized access to, use of, acquisition, disclosure, alteration, or destruction of Discloser's Confidential Information (a "Security Incident"). The notice will describe, to the extent known, the nature of the Security Incident, the information affected, the likely consequences, and the mitigation measures taken or planned.

Recipient will reasonably cooperate with Discloser to investigate, contain, remediate, and mitigate the Security Incident. Dapta will not notify affected individuals or governmental authorities concerning Customer Data without first consulting Customer where legally permitted, unless Applicable Data Protection Law requires Dapta to do so.

8. Required Disclosure and Protected Rights

If Recipient is required by law, regulation, subpoena, or court or governmental order to disclose Confidential Information, Recipient may disclose only the portion legally required and, where legally permitted, will provide Discloser prompt prior written notice and reasonably cooperate, at Discloser's expense, with efforts to obtain protective treatment.

Nothing in this Agreement prohibits a person from making a disclosure protected by Applicable Law, including a good-faith report to a governmental authority or disclosure to that person's attorney for the purpose of reporting or investigating a suspected legal violation.

9. Return and Deletion

Within thirty days after Discloser's written request or the end of the Purpose, Recipient will return or securely delete Discloser's Confidential Information, including copies held in AI Tools under Recipient's control, and, upon request, certify completion in writing. Recipient may retain copies required by law, copies maintained in routine backup systems, and records necessary to establish compliance, provided that retained copies remain subject to this Agreement, are not used for any other purpose, and are deleted according to Recipient's ordinary retention cycle.

Dapta will direct its subprocessors to return or delete Customer Confidential Information. Backup copies will be deleted or overwritten within ninety days after the end of the applicable backup cycle, unless a longer period is required by law. While Dapta provides services under a separate written agreement, Customer Data will be retained and deleted as that agreement and any applicable DPA provide.

10. No Warranty; No Obligation to Proceed

Confidential Information is provided "AS IS," without warranty of any kind, express or implied, including as to its accuracy, completeness, or performance, except as expressly provided in a separate written agreement between the Parties. Nothing in this Agreement obligates either Party to disclose any particular information or to enter into any further agreement or transaction.

Neither Party is restricted from developing, acquiring, or marketing products or services that compete with the other Party's products or services, provided it does so without using or disclosing the other Party's Confidential Information. This Section does not grant either Party permission to use Customer Data, Personal Data, or trade secrets in developing a competing product.

11. Duration and Survival

This Agreement continues until either Party ends it by written notice. Recipient's obligations for Confidential Information disclosed before termination continue for three years after termination. Obligations concerning trade secrets continue for so long as the information remains a trade secret under Applicable Law. Obligations concerning Personal Data, credentials, security materials, and Customer Data continue until the information is deleted or returned, except for legally retained copies, which remain protected for as long as retained.

12. Remedies

Unauthorized use or disclosure of Confidential Information may cause irreparable harm for which monetary damages may be inadequate. Discloser may seek injunctive or other equitable relief against any actual or threatened breach, without posting a bond where the law permits, in addition to any other available remedies. This Section does not waive any requirement to arbitrate monetary disputes under Section 13.

13. Governing Law and Dispute Resolution

This Agreement is governed by the laws of the State of Delaware, without regard to its conflict-of-law rules.

Except for a request for injunctive or other equitable relief under Section 12, any dispute arising out of or relating to this Agreement will be finally resolved by confidential arbitration under the UNCITRAL Arbitration Rules by one arbitrator. The seat of arbitration will be Wilmington, Delaware, USA. The arbitration will be conducted in English, and hearings may be conducted remotely unless the arbitrator determines that an in-person hearing is necessary.

The Parties will share the arbitrator's fees and administrative costs equally, subject to the arbitrator's authority to reallocate those costs in the final award. Each Party will bear its own legal fees unless the arbitrator determines that an award of fees is permitted by Applicable Law and justified by the circumstances. Nothing prevents either Party from seeking interim or injunctive relief in a court of competent jurisdiction to protect Confidential Information, Personal Data, or intellectual property, or to compel or enforce arbitration.

14. Notices and Electronic Signatures

Notices under this Agreement must be in writing and are effective when delivered by email to Dapta at **admin@daptatech.com** and to Customer at the work email provided in the signature block below. Either Party may change its notice address by written notice.

The Parties consent to electronic records and signatures under the U.S. Electronic Signatures in Global and National Commerce Act, the Uniform Electronic Transactions Act, and other applicable electronic-signature laws. Each signatory represents that they have authority to bind the Party for which they sign. This Agreement may be signed in counterparts, including electronically, each of which is deemed an original.

15. Assignment and General Terms

Neither Party may assign this Agreement without the other Party's prior written consent, except to an Affiliate or successor in a merger, reorganization, or sale of all or substantially all of the assets or business to which this Agreement relates, provided that the successor is bound by this Agreement. The Parties are independent contractors. Each Party represents that it has full power and authority to enter into this Agreement and that this Agreement is binding on it.

No waiver is effective unless in writing, and failure to enforce any provision is not a waiver. If any provision is held unenforceable, it will be limited to the minimum extent necessary and the remaining provisions will remain in effect. Neither Party may amend this Agreement except in a writing signed by both Parties.

This Agreement is the entire agreement between the Parties concerning its subject matter, except that an applicable services agreement or DPA controls where expressly stated in Sections 3, 4, and 9. This Agreement does not limit any rights a Party has under trade-secret, copyright, patent, or other Applicable Law. Any translation is provided for convenience only; the English-language version controls.

END OF DOCUMENT