DOCUMENT RECORD

VERSION	EFFECTIVE	GOVERNING TEXT
2026-10-15	October 15, 2026	English

REFERENCE
legal.dapta.ai/en/documents/privacy-policy

Global Privacy Policy

Last Updated: October 15, 2026

1. Introduction and Scope

This Privacy Policy describes how Dapta, Inc. (“Dapta,” “we,” “us,” or “our”) collects, uses, discloses, stores, transfers, and otherwise processes Personal Information when you visit our websites, interact with our marketing activities, communicate with us, request information or support, create or use an account, access or use our artificial intelligence-powered platform, or otherwise interact with us.

Dapta provides a business-to-business software platform that enables customers to create, configure, deploy, and manage AI-powered voice and text agents, automated workflows, communications, integrations, and related functionality. Depending on how a customer configures the Services, Dapta-powered agents may interact with individuals through inbound or outbound telephone calls, SMS, WhatsApp, web chat, email, or other communication channels; connect with customer relationship management (“CRM”) systems, calendars, APIs, databases, and other third-party applications; process conversational inputs; qualify leads; schedule appointments; perform follow-up communications; update connected systems; generate summaries or insights; and perform other customer-configured tasks.

Our websites, platform, AI agents, applications, APIs, integrations, communications tools, professional services, and related products and services are collectively referred to in this Privacy Policy as the “Services.”

This Privacy Policy applies to Personal Information processed by Dapta in connection with the Services. It also describes, at a general level, how Dapta processes Personal Information on behalf of its business customers. It does not replace any customer-specific privacy notice that may apply when a business uses Dapta to communicate with or process information about its own customers, prospects, employees, candidates, or other individuals.

The jurisdiction-specific disclosures supplement this Privacy Policy and apply only to the extent that the laws of the relevant jurisdiction govern the applicable processing. If a jurisdiction-specific disclosure conflicts with this global policy, the jurisdiction-specific disclosure controls to the extent required by applicable law.

2. Our Role in Processing Personal Information

Dapta processes Personal Information in two principal capacities.

2.1 Personal Information Processed for Dapta's Own Business Purposes

When Dapta determines the purposes and means of processing Personal Information for its own business purposes—for example, in operating its websites, administering accounts and subscriptions, supporting Customers, conducting sales and marketing, securing the Services, analyzing product usage, and complying with applicable law—Dapta acts as a controller, business, or similar regulated entity under applicable law. The purposes for which Dapta processes this information are described in Section 6.

2.2 Individuals Interacting with Dapta-Powered Agents

If you interact with a Dapta-powered AI agent, website widget, workflow, or other implementation that is operated on behalf of a Customer, the Customer generally determines the purpose for which your Personal Information is processed.

3. Definitions

Customer: a business or organization that purchases, accesses, or uses the Services.

Customer Data: information submitted to, stored in, transmitted through, generated through, or otherwise processed by the Services on behalf of a Customer.

Customer Content: the substantive content a Customer or its authorized users submit to or generate through the Services, including communications, prompts, files, knowledge-base materials, recordings, transcripts, messages, instructions, and other content.

End User: an individual who interacts with a Customer through the Services, including through a Dapta-powered voice agent, text agent, web chat, workflow, or other communication channel.

Personal Information: information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked to an identified or identifiable individual, as defined by applicable law.

Communications Data: information processed in connection with voice, text, email, chat, WhatsApp, or other communications facilitated through the Services.

4. Personal Information We Collect and Process

The Personal Information we process varies depending on how you interact with Dapta, the Services you use, and how those Services are configured.

4.1 Information You Provide Directly to Dapta

Dapta may ask you to provide Personal Information when you create an account, request a demonstration, purchase or use Services, submit a form, communicate with sales or support, participate in a survey or event, provide feedback, or otherwise interact directly with Dapta. The categories of Personal Information you may provide to us include, but are not limited to:

i. Email address

ii. First name and last name

iii. Government ID, business registration, address information, where required for business verification

iv. Phone number

v. Address, State, Province, ZIP/Postal code, City

vi. Company or organization name

vii. Job title

viii. Payment and billing information

ix. Customer account information

x. Customer content, feedback, surveys or questionnaires

xi. Communications between you and Dapta, including emails, support, communications, recorded calls, and related transcripts, where applicable.

xii. Language and communication preferences;

xiii. Other information you choose to provide.

4.2 Customer Data

Depending on the Customer's business and configuration, Customer Data may include:

i. Names, phone numbers, email addresses, and other contact information;

ii. Lead, prospect, customer, and CRM records;

iii. Contact lists and sales information;

iv. Customer-service records and support information;

v. Appointment, scheduling, and calendar information;

vi. Forms, responses, notes, and conversation history;

vii. Candidate, employee, contractor, or applicant-related information;

viii. Account, transaction, collection, or business-process information;

ix. Documents, FAQs, websites, knowledge-base materials, and other Customer-provided reference content;

x. Data imported through APIs, databases, spreadsheets, or integrations; and

xi. Other information selected by the Customer for processing through the Services.

Because Customers determine how they configure the Services, Dapta does not independently determine all categories of Customer Data that may be submitted to or generated through the platform.

4.3 AI Communications — Voice, Text, Chat, and Other Communications

Dapta's Services may facilitate communications between Customers and End Users through AI-powered voice and text agents and other communications functionality. Dapta may collect and process the following types of data, among others:

i. Audio or voice communications;

ii. Call recordings, where recording functionality is used;

iii. Call or conversation transcripts;

iv. Conversation summaries;

v. SMS, WhatsApp, webchat, or other message content;

vi. Email content where an applicable integration or workflow is enabled;

vii. Sender and recipient identifiers, including telephone numbers;

viii. Communication date, time, duration, status, and delivery information;

ix. Telecommunications, carrier, routing, source, and destination information;

x. Call or message logs and interaction history;

xi. End User inputs and agent responses;

xii. Structured information extracted from a conversation; and

xiii. Other information generated through or necessary to provide the relevant communication.

4.4 AI Interaction, Prompt, and Workflow Data

Depending on how a Customer configures and uses the Services, Dapta may process information relating to AI interactions, agent configuration, and workflow execution, including:

i. Prompts and instructions;

ii. Agent names, descriptions, configurations, and system instructions;

iii. Customer-defined workflows and actions;

iv. End User inputs and AI-generated outputs;

v. Conversation context and memory used for the applicable interaction;

vi. Knowledge-base queries and retrieved information;

vii. Workflow execution data and API events;

viii. Classifications, structured fields, summaries, and outcome data;

ix. Agent performance and quality information; and

x. Related logs.

4.5 Integrations and Connected Services

Customers may connect Dapta to CRM (Customer Relationship Management) systems, calendars, communication services, telephony providers, messaging platforms, email services, videoconferencing tools, databases, spreadsheets, productivity applications, customer-support tools, or other third-party software. When an integration is enabled, Dapta may receive, access, transmit, modify, or write back information as necessary to provide the requested functionality.

The information available through an integration depends on the third-party provider, the permissions granted, the Customer's configuration, and the functionality requested. Dapta may also process technical credentials, identifiers, and

settings necessary to establish and maintain the connection with the third-party service.

4.6 Meeting and Calendar Information

When a Customer connects a calendar, scheduling service or meeting-related integration to the Services, Dapta may process information necessary to schedule, manage, or support meetings and appointments, including:

i. Calendar availability and scheduling preferences;

ii. Event dates, times, meeting participants, and meeting titles;

iii. Meeting links and booking information;

iv. Information necessary to create, update, or cancel calendar events; and

v. Where applicable, meeting audio, transcripts, summaries, notes, and action items generated through meeting-related features.

4.7 Usage, Device, and Technical Information

When you access or use the Services, Dapta may automatically collect certain information about your device, browser, and interactions with the Services, including:

i. IP address;

ii. Browser type and settings;

iii. Operating system and device type;

iv. Device or session identifiers;

v. Language, approximate location derived from IP address, and time zone;

vi. Access dates and times;

vii. Pages, links, and features used;

viii. Referral URLs and session information;

ix. Other technical information generated through use of the Services.

4.8 Sensitive Personal Information

Dapta does not require sensitive Personal Information to maintain a standard account. However, depending on a Customer's use case and configuration, Customer Data may include information that is considered sensitive or otherwise subject to heightened protection under applicable law. Where Dapta processes such information on behalf of a Customer, the Customer is responsible for establishing the lawfulness of the underlying processing, and Dapta will process the information in accordance with Customer instructions, applicable agreements, and applicable law.

5. Sources of Personal Information

Dapta may obtain Personal Information from the following sources:

5.1 Directly from You

When you provide your own information to Dapta, for example when you create an account, request a demo, contact us, request support, submit a form, attend an event, or otherwise interact directly with Dapta.

5.2 From Customers

When Customers provide information about other individuals through the Services, for example by uploading contact information, importing lead or customer records, or connecting third-party systems that contain Personal Information.

5.3 Through Communications and AI Interactions

Information may be received or generated when an individual speaks, messages, chats, submits information, or otherwise interacts with a Dapta-powered agent, workflow, meeting feature, or communication channel.

5.4 Automatically

Dapta may collect certain technical and usage information automatically when you visit our websites, use the Services, or interact with our electronic communications, including through cookies, similar technologies, and server or application logs. The categories of information collected in this manner are described in Section 4.7, and Dapta's use of cookies and similar technologies is described in Section 11.

5.5 From Connected Third-Party Services

We may obtain Personal Information from third parties that support, integrate with, or otherwise interact with the Services. Where appropriate, we may combine this information with information collected directly from you or generated through your use of the Services.

The information we receive depends on the third party involved, the permissions granted, the features used, and the nature of the relevant integration or business relationship. These third-party sources may include:

i. **Telecommunications carriers and service providers.** We may receive information necessary to support and route communications, such as carrier information, phone number validation, portability information, routing data, call delivery status, and related network or traffic records.

ii. **Communications and messaging providers.** Where the Services rely on third-party communications infrastructure, we may receive call or message metadata, source and destination information, connection and delivery status, and other technical information generated in connection with the transmission of communications.

iii. **Analytics and marketing providers.** We may receive information concerning interactions with Dapta's marketing activities, advertisements, or campaigns, such as clicks, impressions, conversion events, campaign attribution information, and advertising identifiers, where applicable.

iv. **Social media and online platforms.** If you interact with Dapta through a social media platform or other online service, we may receive information made available to us through that platform in accordance with your settings and the platform's applicable terms.

v. **Business and professional data providers.** We may obtain business-related information, such as company name, employer, job title, industry, company size, and professional contact information, for purposes such as sales, business development, lead generation, and maintaining business records.

vi. **Payment and billing providers.** Where third-party payment processors support paid Services, we may receive information such as billing verification details, payment status, transaction confirmations, and related

payment-processing information.

vii. **Connected applications and integrations.** When an authorized user connects a third-party application or service to Dapta, we may receive information from that service to the extent permitted by the user's authorization and necessary to provide the requested integration or functionality.

6. How We Use Personal Information

Dapta may use Personal Information for the purposes described below, depending on how you interact with Dapta and how Customers use the Services.

6.1 Providing and Operating the Services

Dapta may use Personal Information as necessary to provide, operate, and support the Services, including:

i. Create and maintain accounts and authenticate users;

ii. Provide access to the platform;

iii. Configure and operate AI agents and workflows;

iv. Enable inbound and outbound voice communications;

v. Send, receive, and process text or chat communications;

vi. Generate responses and process End User inputs;

vii. Record, transcribe, or summarize communications where enabled;

viii. Extract, classify, route, or structure information;

ix. Schedule appointments and manage calendar events;

x. Update connected CRM, ATS, database, or other systems;

xi. Synchronize data between integrations;

xii. Enable human handoff or escalation;

xiii. Execute customer-configured workflows and API actions; and

xiv. Otherwise provide the functionality requested by the Customer.

6.2 Customer Support and Service Administration

Dapta may use Personal Information to provide customer support and administer its relationship with Customers, including to:

i. Respond to questions and support requests;

ii. Investigate problems and troubleshoot errors;

iii. Review support interactions;

iv. Communicate regarding incidents, updates, or service status;

v. Administer subscriptions, billing, users, and workspaces; and

vi. Maintain records of the commercial relationship.

6.3 Security, Integrity, and Abuse Prevention

Dapta may use Personal Information to protect the security and integrity of the Services and prevent fraud, abuse, or unauthorized activity, including to:

i. Authenticate users and protect accounts;

ii. Detect unauthorized activity, fraud, spam, or misuse;

iii. Monitor and investigate security incidents;

iv. Enforce usage restrictions and policies;

v. Protect infrastructure and platform integrity; and

vi. Protect Dapta, Customers, End Users, and others.

6.4 Analytics, Development, and Service Improvement

Dapta may use Personal Information to understand how the Services are used, measure performance, identify and resolve errors, improve reliability and usability, evaluate existing features, and develop new functionality. Any use of Customer Data for service-improvement or AI-related purposes is subject to the applicable Customer agreement and the disclosures in Section 7.

6.5 Communications With You

Dapta may use Personal Information to communicate with you about the Services and its relationship with you or your organization, including to send account and service notifications, security notices, billing and subscription communications, support messages, product or feature announcements, administrative or legal notices, and other communications necessary to maintain the relationship with you or your organization.

6.6 Marketing and Business Development

Where permitted by applicable law, Dapta may use Personal Information to respond to sales inquiries, conduct business development, provide information about the Services, send newsletters and product announcements, and invite individuals to demonstrations, surveys, or events.

6.7 Legal, Regulatory, and Corporate Purposes

Dapta may use Personal Information as necessary to comply with legal obligations, protect its rights and interests, and support its corporate operations, including to:

i. Comply with applicable law and legal obligations;

ii. Respond to lawful governmental or legal requests;

iii. Enforce contracts, terms, and policies;

iv. Investigate suspected violations, fraud, or misuse;

v. Establish, exercise, or defend legal claims;

vi. Protect rights, property, systems, or safety;

vii. Perform audits, accounting, financial reporting, and corporate governance; and

viii. Support an actual or proposed corporate transaction.

7. Artificial Intelligence and Automated Processing

Artificial intelligence and machine-learning technologies are integral to certain Dapta Services. Depending on a Customer's configuration, AI-powered functionality may be used to understand natural-language voice or text inputs, generate conversational responses, transcribe or summarize communications, extract structured information, classify or prioritize interactions, qualify leads, identify stated intent, route inquiries, retrieve information from Customer-provided knowledge sources, initiate workflows, schedule appointments, update connected systems, generate follow-up communications, or perform other Customer-configured functions.

7.1 Customer Control and Responsibility

Customers determine how their Dapta agents and workflows are configured and the business purposes for which they are deployed. Customer responsibilities relating to Customer Data and use of the Services are described in Section 10.

7.2 Profiling and Automated Decisions

Certain Customer-configured workflows may classify, score, prioritize, route, or otherwise evaluate interactions based on information provided through the Services. Where applicable privacy law provides rights relating to automated decision-making or profiling, those rights may apply depending on the specific use case and nature of the processing. Where Dapta performs such processing solely on behalf of a Customer, the Customer generally determines the purpose and essential parameters of the processing.

7.3 Third-Party AI and Speech Providers

Dapta may use third-party artificial-intelligence, machine-learning, speech-recognition, text-to-speech, natural-language-processing, or large-language-model providers to provide particular features of the Services. When a feature requires interaction with such a provider, information necessary to provide the feature may be transmitted to that provider, subject to applicable contractual, security, and legal requirements.

7.4 Use of Customer Data for Model Training

Dapta does not use Customer Data or Customer Content, including recordings, transcripts, prompts, and messages, to train or fine-tune artificial intelligence or machine-learning models that are made available to other customers or third parties, unless the relevant Customer has expressly authorized such use in writing. Dapta may use Customer Data to configure, evaluate, and improve the performance of the Services as provided to the relevant Customer, in accordance with the applicable Customer agreement.

Dapta may also use information that has been aggregated, anonymized, or de-identified in accordance with Section 19 for model training, evaluation, analytics, or service improvement purposes.

Dapta may also use third-party artificial intelligence or machine-learning providers in connection with these activities. Where Customer Data is provided to such providers, Dapta will do so subject to applicable contractual, confidentiality, security, and data-protection requirements, including restrictions that prohibit such providers from using Customer Data to train or improve models made available to others.

Where Customer authorization or consent is required by applicable law or contract, Dapta will obtain such authorization before using Customer Data for these purposes.

Google Workspace API data is subject to the separate limitations described in Section 12.

8. Voice Calls, Messaging, Call Recording and Transcription

Because Dapta enables Customers to communicate with End Users through multiple channels, communications may be subject to privacy, telecommunications, marketing, consumer-protection, call-recording, and consent laws that vary by jurisdiction.

8.1 Voice Calls

Customers may use the Services to make or receive AI-powered voice calls. Dapta may process telephone numbers, audio, telephony metadata, transcripts, agent outputs, conversation results, and other information necessary to provide the call.

8.2 Recording and Transcription

When a Customer enables recording or transcription features, Dapta may process the resulting information to provide those features. Customers are responsible for ensuring that any required notices are provided and any required consents are obtained before using recording or transcription features.

8.3 SMS, WhatsApp, Email, and Other Messaging

Customers may use Dapta to send or receive SMS, WhatsApp, webchat, email, or other messages. The use of these channels may be subject to laws and platform rules concerning consent, marketing, opt-outs, message frequency, sender identification, and permissible content. Customers are responsible for complying with requirements governing communications they initiate through the Services.

9. How We Disclose Personal Information

Dapta may disclose Personal Information in the circumstances described below.

9.1 Service Providers and Subprocessors

Dapta may engage third parties to support cloud hosting, computing infrastructure, databases, storage, AI and machine-learning technology, speech processing, telecommunications, messaging, email, analytics, cybersecurity, authentication, monitoring, customer support, CRM services, payment processing, billing, and other technology or professional functions. Providers receive Personal Information only to the extent reasonably necessary to provide their services or for another permitted purpose.

9.2 AI Providers

Where necessary to enable AI functionality selected by a Customer, Dapta may transmit relevant information to AI or machine-learning providers. Depending on the feature, this may include prompts, instructions, portions of Customer Content, conversation context, audio, transcripts, or other information necessary to generate the requested output.

9.3 Telecommunications and Messaging Providers

Dapta may disclose Communications Data and related metadata to telephone carriers, messaging providers, communications platforms, aggregators, and infrastructure providers where necessary to deliver or support

communications.

9.4 Legal and Regulatory Disclosures

Dapta may disclose Personal Information where it reasonably believes disclosure is necessary to comply with applicable law or valid legal process; respond to lawful governmental requests; investigate fraud, misuse, or security incidents; enforce agreements; protect legal rights or safety; or establish, exercise, or defend legal claims. Where legally permitted and appropriate, Dapta may notify the affected Customer before disclosing Customer Data in response to legal process.

9.5 Corporate Transactions

Personal Information may be disclosed in connection with an actual or proposed merger, financing, acquisition, investment, reorganization, restructuring, bankruptcy, sale of assets, or similar corporate transaction, subject to applicable confidentiality and legal requirements.

9.6 Affiliates

Where applicable, Dapta may disclose Personal Information to its parent companies, subsidiaries, or other affiliated entities where reasonably necessary for business administration, finance, legal and compliance matters, security, customer support, or operation of the Services, subject to applicable law and appropriate safeguards.

10. Customer Responsibilities for Customer Data

Customers determine the purposes for which Customer Data is submitted to and processed through the Services. Customers are responsible for ensuring that their collection and use of Customer Data, their communications with End Users, and their instructions to Dapta comply with applicable law, including applicable notice and consent requirements. Dapta processes Customer Data in accordance with Customer instructions, applicable agreements, and applicable law.

11. Cookies and Similar Technologies

Dapta's websites and Services may use cookies and similar technologies for essential functionality, authentication, preferences, security, analytics, performance, troubleshooting, and, where applicable and permitted by law, marketing or advertising measurement.

Users may be able to control certain cookies through a preference tool made available on Dapta's website, browser or device settings, or other legally required choice mechanisms. Disabling certain essential technologies may affect functionality.

12. Google and Microsoft Authentication and Connected Services

Dapta allows users to create or access their accounts using Google or Microsoft authentication. Depending on the functionality authorized by the user, Dapta may receive basic account information for authentication purposes and may access information from connected services as necessary to provide the requested functionality.

Dapta uses information received through these integrations only to provide, maintain, secure, or support the functionality authorized by the user and as otherwise permitted by applicable provider requirements.

Dapta retains information obtained through these integrations only for as long as reasonably necessary to provide the applicable functionality or as otherwise required or permitted by applicable law.

13. Data Retention and Deletion

Dapta retains Personal Information only for as long as reasonably necessary to fulfill the purposes for which the information was collected or processed, unless a longer retention period is required or permitted by applicable law.

When Personal Information is no longer required, Dapta will delete, anonymize, de-identify, aggregate, or securely dispose of it.

14. Information Security

Dapta maintains administrative, technical, and organizational safeguards designed to protect Personal Information against unauthorized access, loss, misuse, alteration, disclosure, or destruction. These safeguards may include access controls, authentication measures, encryption, monitoring, security testing, incident-response procedures, and other measures appropriate to the nature of the information and Services.

Dapta has completed a SOC 2 Type II examination covering the Dapta Platform.

No method of electronic transmission or storage is completely secure. Customers are responsible for maintaining appropriate security over credentials, passwords, API keys, connected accounts, integrations, devices, and user permissions within their control.

15. International Data Processing and Transfers

Dapta provides Services to Customers in multiple countries and uses service providers and technology providers that may process Personal Information outside the country in which it was originally collected. As a result, Personal Information may be transferred to, stored in, accessed from, or processed in the United States or other countries where Dapta's service providers operate.

Privacy and data-protection laws may differ between countries. Where applicable law requires specific safeguards for international transfers of Personal Information, Dapta will implement appropriate measures in accordance with applicable legal requirements.

Where Dapta processes Customer Data on behalf of a Customer, additional terms governing international data transfers may be included in the applicable Customer agreement or data processing agreement.

16. Third-Party Sites, Services and Integrations

Dapta's websites and Services may contain links to or integrations with third-party websites, applications, services, and platforms. Dapta does not control the independent privacy practices of third parties. Where a Customer or user chooses to interact directly with a third-party service, Personal Information processed independently by that third party is subject to the third party's own privacy policy and legal terms.

17. Privacy Rights and Choices

Depending on your location, the applicable law, and Dapta's role in processing the relevant information, you may have rights concerning your Personal Information. These rights may include the right to:

i. Know whether Personal Information is being processed;

ii. Request access to or a copy of Personal Information;

iii. Correct or update inaccurate or incomplete information;

iv. Request deletion, suppression, or cancellation;

v. Object to or restrict certain processing;

vi. Withdraw or revoke consent where legally applicable;

vii. Limit certain uses or disclosures;

viii. Opt out of certain marketing communications;

ix. Opt out of certain sale, sharing, or targeted-advertising practices;

x. Obtain data portability where applicable;

xi. Obtain information about certain automated processing;

xii. Challenge or opt out of certain automated decisions or profiling where applicable;

xiii. Appeal certain privacy-request decisions where provided by law; and

xiv. Submit a complaint to a competent privacy or data-protection authority.

17.1 Requests Relating to Dapta's Own Processing

If Dapta processes your Personal Information for its own purposes, you may submit a request using the contact information in Section 21. Dapta may request information reasonably necessary to verify your identity or authority before fulfilling certain requests.

17.2 Marketing Choices

You may unsubscribe from promotional email through the unsubscribe link included in the message. You may continue to receive non-promotional communications required to provide or administer the Services.

18. Children's Privacy

Dapta's Services are not directed to children, but if Dapta becomes aware that Personal Information relating to a child has been collected or processed in violation of applicable law, Dapta will take appropriate steps to delete or otherwise address the information, as required by applicable law and, where applicable, in accordance with the relevant Customer's instructions and contractual obligations.

19. De-Identified and Aggregated Information

Dapta may create information that has been aggregated or de-identified so that it cannot reasonably be used to identify a particular individual. Subject to applicable law and Customer agreements, Dapta may use such information for analytics, service improvement, security, capacity planning, research, statistical analysis, and business planning.

Where applicable law requires Dapta to maintain information in de-identified form, Dapta will take reasonable measures designed to prevent re-identification and will not attempt to re-identify the information except as permitted by law.

20. Changes to this Privacy Policy

Dapta may update this Privacy Policy from time to time to reflect changes in its practices or the Services. When Dapta makes changes, it will update the “Last Updated” date at the top of this Privacy Policy and post the updated version on its website. If the changes are material, Dapta will provide additional notice, such as by email to the account holder or through a notice within the Services, before the changes take effect.

21. Contact Us and Privacy Requests

If you have questions, concerns, or requests relating to this Privacy Policy or Dapta’s privacy practices, please contact:

- **Company:** Dapta, Inc.
- **Legal Department:** legal@daptatech.com

Jurisdiction-Specific Privacy Disclosures

The following disclosures apply only where the relevant jurisdiction’s privacy law governs the processing. The global provisions remain applicable except to the extent a local disclosure provides otherwise.

22. United States Privacy Disclosures

Residents of certain U.S. states may have additional rights under state privacy laws. The availability and scope of those rights depend on the state, the nature of the processing, statutory thresholds and exemptions, and whether Dapta acts for its own purposes or solely as a service provider or processor for a Customer.

22.1 State Privacy Rights

Depending on applicable state law, eligible individuals may have rights to know or access Personal Information; correct inaccuracies; request deletion; obtain a portable copy; opt out of sale, sharing, targeted advertising, or certain profiling; limit certain uses of sensitive Personal Information; appeal certain privacy-request decisions; and receive non-discriminatory treatment for exercising privacy rights.

22.2 Customer Data

Where Dapta processes Personal Information solely as a processor, service provider, or contractor for a Customer, applicable state privacy law may require the Customer rather than Dapta to respond directly to consumer requests. Dapta will provide assistance as required by applicable law and contract.

23. Additional Privacy Notice for Mexico

This Section applies to Personal Information subject to Mexico’s Federal Law on the Protection of Personal Data Held by Private Parties and other applicable Mexican data protection requirements. This Section supplements the general provisions of this Privacy Policy with additional information applicable to Personal Information processed by Dapta in Mexico. If there is any conflict between this Section and the general provisions of this Privacy Policy, this Section will control to the extent required by Mexican law.

23.1 Identity and Address of the Responsible Party

Where Dapta determines the purposes and means of processing, the responsible party is Dapta, Inc., a Delaware corporation. Contact: Legal Department, legal@daptatech.com.

23.2 Categories of Personal Data

Depending on the interaction, Dapta may process identification data; contact data; business and professional information; account and authentication information; billing and commercial information; technical and usage data; Communications Data; audio recordings; transcripts; messaging content; AI interaction data; integration data; and other Customer Data described in Section 4.

Customer Data may contain sensitive Personal Data where a Customer chooses to process such information. Where Dapta acts as Responsible and directly processes sensitive Personal Data, Dapta will apply any additional consent and processing requirements required by Mexican law.

23.3 Primary Purposes

Primary purposes may include providing the Services; creating and administering accounts; authenticating users; operating AI-agent and workflow functionality; processing communications; maintaining integrations; providing support; billing; security and fraud prevention; administering the contractual relationship; complying with legal obligations; and protecting Dapta's legal rights. Where Dapta processes Customer Data as a service provider, the Customer generally determines the underlying purposes.

23.4 Secondary Purposes

Dapta may also use business contact information for purposes that are not necessary to provide the Services, such as marketing communications, product updates, surveys, events, and other promotional activities, where permitted by law.

Individuals may refuse or request that Dapta cease these secondary uses by contacting legal@daptatech.com.

23.5 Limiting Use or Disclosure

Where legally applicable, individuals may request limitations on certain uses or disclosures of Personal Data by contacting Dapta. The request should identify the individual, the Personal Data concerned, and the use or disclosure the individual seeks to limit.

23.6 ARCO Rights

Subject to applicable Mexican law, individuals may exercise rights of Access, Rectification, Cancellation, and Opposition ("ARCO Rights"). Access concerns the Personal Data held and conditions of processing; Rectification permits correction of inaccurate or incomplete data; Cancellation permits cancellation or deletion where legally appropriate; and Opposition permits objection to processing in circumstances recognized by law. Individuals may also request revocation of consent to the extent permitted by law.

23.7 ARCO Request Procedure

A request should contain information reasonably sufficient to identify the individual, provide a means to receive communications, verify identity or representation, clearly describe the Personal Data concerned, identify the right being exercised, describe the requested action, and provide information reasonably useful to locate the Personal Data. For rectification, the requester should identify the correction sought and, where applicable, provide supporting documentation.

Requests may be submitted to legal@daptatech.com. Subject to applicable law, Dapta will communicate its determination within the legally prescribed period and, if the request is granted, implement the applicable action within the period required by law. The currently applicable statutory framework generally provides twenty (20) days to communicate a determination and fifteen (15) days to implement an approved request, subject to lawful extensions and

exceptions.

23.8 Revocation of Consent

Where processing is based on consent and Mexican law permits revocation, an individual may request revocation by contacting Dapta. Revocation generally does not apply retroactively and may not be available where processing remains necessary or permitted under another legal basis or exception. Revocation may affect Dapta's ability to provide functionality that depends on the relevant Personal Data.

23.9 Transfers and Service-Provider Processing

Dapta may communicate Personal Data to technology, infrastructure, communications, AI, security, analytics, payment, and professional-service providers acting on its behalf. Where the provider processes Personal Data on Dapta's behalf and under Dapta's instructions, the relationship may be treated differently under Mexican law from a transfer to an independent third party. Dapta may also transfer Personal Data to independent third parties where required or permitted by law, necessary to maintain or fulfill a legal relationship, connected to legal proceedings or a corporate transaction, or otherwise permitted with any required consent.

Personal Data may be processed or stored outside Mexico, including where Dapta's providers or infrastructure are located outside Mexico. International processing will be handled in accordance with applicable Mexican law.

24. Additional Privacy Information for Colombia

This Section applies to Personal Data subject to Colombia's Law 1581 of 2012, Decree 1074 of 2015, the applicable provisions of Title V of the Superintendence of Industry and Commerce's Single Circular, and other applicable Colombian data protection requirements. This Section supplements the general provisions of this Privacy Policy with additional information applicable to Personal Data processed in Colombia. If there is any conflict between this Section and the general provisions of this Privacy Policy, this Section will control to the extent required by applicable Colombian law.

24.1 Data Controller and Processor Roles

Under Colombian law, Dapta may act as a data controller when it determines the purposes and means of processing Personal Data, or as a data processor when it processes Personal Data on behalf of and according to the instructions of a Customer.

Where Dapta acts solely as a data processor, the relevant Customer generally acts as the data controller and is responsible for determining how requests from Data Subjects are handled. Dapta will provide assistance where required by applicable law or its contractual obligations.

24.2 Authorization

Where Dapta acts as a data controller and authorization is required under Colombian law, Dapta will obtain or rely on an appropriate authorization before processing Personal Data. The authorization will provide the Data Subject with information about the purposes for which the Personal Data will be processed.

Where Colombian law provides an exception to the authorization requirement, Dapta may process Personal Data in accordance with that exception.

Where Dapta acts solely as a data processor, the Customer is generally responsible for obtaining any required authorization or otherwise establishing the lawful basis necessary for the Customer's processing of Personal Data.

24.3 Rights of Data Subjects

Subject to applicable Colombian law, Data Subjects may have the right to access, know, update, and correct their Personal Data; request evidence of authorization where legally applicable; obtain information about how their Personal Data has been used; request deletion of Personal Data where legally permitted; revoke authorization where legally permitted; submit inquiries and complaints regarding the processing of their Personal Data; and file a complaint with the Superintendence of Industry and Commerce after satisfying any applicable procedural requirements.

24.4 Inquiries

A Data Subject or other legally authorized person may submit an inquiry regarding Personal Data processed by Dapta as a data controller by contacting legal@daptatech.com.

Dapta will respond to the inquiry within ten (10) business days from the date it is received. If Dapta is unable to respond within that period, it will inform the requesting person of the reason for the delay and indicate the date by which the inquiry will be addressed, which will not exceed five (5) additional business days.

Where the request concerns Customer Data processed by Dapta on behalf of a Customer, Dapta may direct the request to the relevant Customer or assist the Customer in responding, as appropriate.

24.5 Complaints

A Data Subject or other legally authorized person who believes that Personal Data should be corrected, updated, or deleted, or that applicable data protection obligations have not been complied with, may submit a complaint. The complaint should identify the Data Subject, describe the relevant facts, provide contact information, describe the action requested, and include any supporting documentation relevant to the request.

If the complaint is incomplete, Dapta may request additional information within five (5) days of receipt. If the requested information is not provided within two (2) months from the date of that request, the complaint may be treated as withdrawn.

A complete complaint will be addressed within fifteen (15) business days beginning on the day following receipt. If Dapta is unable to respond within that period, it will inform the requesting person of the reason for the delay and the date by which the complaint will be addressed, which will not exceed eight (8) additional business days.

Where Dapta acts as a data processor and is not responsible for resolving the complaint, it may forward the complaint to the relevant Customer or other competent data controller and assist with the response as required by applicable law or contractual obligations.

24.6 Complaints to the Superintendence of Industry and Commerce

Where applicable, the Data Subject may file a complaint to the Superintendence of Industry and Commerce after completing the consultation or claim procedure before the relevant data controller or data processor, as required by Colombian law.

24.7 International Transfers and Transmissions

Dapta may use servers, infrastructure, affiliates, and service providers located outside Colombia. Where Dapta communicates Personal Data outside Colombia, the arrangement may constitute an international “transfer” (transferencia) or “transmission” (transmisión) depending on the role of the recipient and the nature of the processing. Dapta will handle international transfers and transmissions in accordance with applicable Colombian requirements, including requirements applicable to processing and restrictions applicable to transfers to other data controllers.

24.8 Sensitive Data and Minors

Where Personal Data is considered sensitive under Colombian law, Dapta will apply applicable heightened requirements. Where Dapta acts solely as a data processor for Customer Data, the Customer is responsible for determining whether sensitive-data processing is lawful and whether additional authorization or disclosures are required. Processing of Personal Data concerning children or adolescents will be handled in accordance with applicable Colombian requirements and the best interests and fundamental rights of the minor.

24.9 Contact Information and Area Responsible for Requests

Dapta, Inc. may be contacted at legal@daptatech.com. Dapta's Legal Department is responsible for handling inquiries and complaints from Data Subjects.

24.10 Effective Date

This Privacy Policy is effective as of the "Last Updated" date indicated above. Personal Data will remain in Dapta's databases for as long as reasonably necessary to fulfill the purposes described in this Privacy Policy, in accordance with Section 13.

END OF DOCUMENT