Data Processing Agreement

Justido Solutions — AI Receptionist

Auftragsverarbeitungsvertrag (AVV)

pursuant to Article 28 GDPR (EU 2016/679)

based on EU Standard Contractual Clauses 2021/915

B E T W E E N

(the "Controller" or "Client")

A N D

[Justido GmbH] *or* **[Justido LLC]**

see Annex I for the entity executing this DPA

(the "Processor")

each a "Party" and together the "Parties".

> *Note on dual-entity structure: Justido operates through two affiliated legal entities — Justido GmbH (Germany) and Justido LLC (United States). The entity executing this DPA is determined by the Client's jurisdiction, as specified in Annex I, Part A. Each entity acts independently as Processor for its own client contracts; this DPA binds only the executing entity.*

Preamble

This Data Processing Agreement ("DPA") forms an integral part of the underlying services agreement, master services agreement, statement of work, order form, or other contractual relationship between the Parties under which the Processor provides services to the Client (the "Principal Agreement").

This DPA is entered into to comply with Article 28 of Regulation (EU) 2016/679 (the "GDPR") and, where applicable, the UK General Data Protection Regulation and Data Protection Act 2018 ("UK GDPR"), and the Swiss Federal Act on Data Protection ("FADP") (together, "Applicable Data Protection Laws").

In the event of a conflict between this DPA and the Principal Agreement, this DPA prevails with regard to the processing of Personal Data. In the event of a conflict between the body of this DPA and its Annexes, the body prevails unless the Annex expressly states otherwise.

This DPA is drafted in alignment with the Standard Contractual Clauses for controllers and processors adopted by the European Commission pursuant to Article 28(7) GDPR (Commission Implementing Decision (EU) 2021/915 of 4 June 2021). Where Personal Data is transferred outside the European Economic Area, the Parties additionally rely on the Standard Contractual Clauses adopted under Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the "EU Transfer SCCs") and, for UK transfers, the UK International Data Transfer Addendum ("UK IDTA") issued by the Information Commissioner's Office.

1. Definitions

Capitalised terms used in this DPA have the meanings set out below. Terms not defined here take the meanings given to them in the GDPR or the Principal Agreement.

- "Personal Data", "Data Subject", "Processing", "Controller", "Processor" and "Supervisory Authority" have the meanings given in Article 4 GDPR.
- "Client Personal Data" means any Personal Data processed by the Processor on behalf of the Client under the Principal Agreement, as further described in Annex I.
- "Sub-Processor" means any third party engaged by the Processor to process Client Personal Data on the Processor's behalf.
- "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Client Personal Data.
- "Restricted Transfer" means a transfer of Personal Data from the EEA, the United Kingdom or Switzerland to a country that does not benefit from a relevant adequacy decision.
- "Standard Contractual Clauses" or "SCCs" means the EU Transfer SCCs (Commission Implementing Decision (EU) 2021/914).

2. Roles of the Parties and Scope of Processing

With respect to Client Personal Data processed under this DPA, the Client acts as Controller (or, where applicable, as Processor on behalf of a third-party controller) and the Processor acts as Processor (or Sub-Processor, as applicable). The subject-matter, duration, nature and purpose of the processing, the types of Personal Data and categories of Data Subjects are set out in Annex I.

The Processor processes Client Personal Data only on the documented instructions of the Client, including with regard to transfers of Personal Data to a third country, unless required to do so by Union or Member State law to which the Processor is subject. The Principal Agreement, this DPA and the Annexes together constitute the Client's complete and final documented instructions at the effective date. Any additional or alternative instructions must be agreed in writing between the Parties.

If the Processor is of the opinion that an instruction from the Client infringes Applicable Data Protection Laws, it shall inform the Client without undue delay and may suspend performance of the relevant instruction until the Client confirms or modifies it.

3. Obligations of the Processor

3.1 Confidentiality

The Processor ensures that persons authorised to process Client Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Access to Client Personal Data is granted strictly on a need-to-know basis and is revoked promptly upon role change or termination of employment or engagement.

3.2 Security of Processing

The Processor implements and maintains the technical and organisational measures ("TOMs") described in Annex II, designed to ensure a level of security appropriate to the risk in accordance with Article 32 GDPR. The Processor may update the TOMs from time to time provided that the overall level of protection is not materially reduced.

3.3 Assistance to the Client

Taking into account the nature of the processing and the information available, the Processor assists the Client by appropriate technical and organisational measures, insofar as this is possible, in fulfilling the Client's obligations to:

- respond to requests from Data Subjects exercising their rights under Chapter III GDPR (access, rectification, erasure, restriction, portability and objection);
- ensure compliance with Articles 32 to 36 GDPR, including security of processing, notification of Personal Data Breaches, communication of breaches to Data Subjects, data protection impact assessments and prior consultation with Supervisory Authorities.

The Processor shall acknowledge receipt of any Data Subject request forwarded by the Client within two (2) business days, and respond substantively within five (5) business days of receipt, unless additional time is reasonably required due to the complexity or volume of requests, in which case the Processor shall inform the Client of the expected timeline.
The Processor may charge reasonable, documented costs for assistance that materially exceeds ordinary support under the Principal Agreement.

3.4 Personal Data Breach Notification

The Processor shall notify the Client of a Personal Data Breach affecting Client Personal Data without undue delay and, in any event, within seventy-two (72) hours of becoming aware of the Breach. The notification shall, to the extent known at the time and supplemented thereafter as further information becomes available, describe:

- the nature of the Personal Data Breach including, where possible, the categories and approximate number of Data Subjects and Personal Data records concerned;
- the likely consequences of the Breach;
- the measures taken or proposed to address the Breach and mitigate its possible adverse effects;
- the contact point within the Processor from which further information can be obtained.

The Processor shall cooperate with the Client and take reasonable steps to assist in the investigation, mitigation and remediation of the Breach.

3.5 Records of Processing

The Processor maintains written records of all categories of processing activities carried out on behalf of the Client, as required by Article 30(2) GDPR, and makes those records available to the Client and, upon request, to the competent Supervisory Authority.

3.6 Deletion or Return of Personal Data

Upon termination or expiry of the Principal Agreement, or earlier upon the Client's written request, the Processor shall, at the Client's choice, delete or return all Client Personal Data and delete existing copies, unless Union or Member State law requires further storage. Deletion shall be completed within thirty (30) days unless otherwise agreed. Where retained under a legal obligation, the Processor shall continue to protect the Personal Data in accordance with this DPA.

3.7 AI Training and Model Improvement

The Processor and its Sub-Processors shall not use Client Personal Data to train, fine-tune, retrain or otherwise improve artificial-intelligence or machine-learning models, except (a) to the minimum extent technically necessary to provide the Services to the Client at the Client's own instruction, or (b) with the Client's separate, prior, written consent.
Where the Processor's Sub-Processors offer zero-data-retention or opt-out-of-training configurations (including, at the date of this DPA, Retell AI, ElevenLabs, Anthropic and Deepgram), the Processor maintains its accounts under such configurations and shall not opt the Client's data back into training without the Client's prior written consent. This zero-retention / no-training commitment applies to Anthropic both where it is engaged as a sub-sub-processor via Retell AI and under the Processor's separate, direct engagement of Anthropic for its Microsoft 365 assistant.
For the avoidance of doubt, Client Personal Data shall not be used to build, improve or commercialise any general-purpose AI model, foundation model, voice model or speech-recognition model offered by the Processor or any Sub-Processor to third parties.

3.8 AI System Disclosure

Where the Services include AI-enabled voice, chat or other automated interactions with natural persons whose Personal Data is processed under this DPA, the Processor implements AI-system disclosure to those persons in alignment with Article 50 of Regulation (EU) 2024/1689 (the "EU AI Act"), including a clear indication that the person is interacting with an AI system at the point of first interaction, and meaningful information about the AI system's nature and purpose on request.
The Client remains responsible for any additional disclosures required under its own privacy notices and any sector-specific transparency obligations applicable to its business.

4. Sub-Processors

4.1 General Authorisation

The Client hereby grants the Processor general written authorisation, pursuant to Article 28(2) GDPR, to engage Sub-Processors for the provision of the Services. The list of Sub-Processors in effect at the date of this DPA is set out in Annex III.

4.2 Changes to Sub-Processors

The Processor shall inform the Client of any intended addition or replacement of Sub-Processors at least ten (10) business days in advance by updating Annex III and providing notice by email to the Client's designated contact. The Client may object on reasonable data protection grounds within that period; in such case the Parties shall discuss the concerns in good faith, and if no resolution is reached, the Client may terminate the affected Services without liability.

4.3 Flow-Down Obligations

The Processor enters into a written contract with each Sub-Processor that imposes data protection obligations substantially equivalent to those set out in this DPA, in particular providing sufficient guarantees to implement appropriate technical and organisational measures so that the processing meets the requirements of the GDPR. The Processor remains fully liable to the Client for the performance of the Sub-Processor's obligations.

5. International Data Transfers

Where the provision of the Services involves a Restricted Transfer, the Parties agree that such transfer is governed by the appropriate transfer mechanism under Applicable Data Protection Laws, in the following order of precedence:

- a valid adequacy decision of the European Commission (or equivalent UK or Swiss decision) covering the destination country;
- the EU Transfer SCCs (Module 2 — Controller-to-Processor, or Module 3 — Processor-to-Processor, as applicable), which are hereby incorporated by reference and deemed entered into between the Parties, with the options and specifications set out in Annex IV;
- for transfers subject to UK data protection law, the UK IDTA as set out in Annex IV;
- for transfers subject to Swiss law, the SCCs adapted in accordance with guidance issued by the Swiss Federal Data Protection and Information Commissioner.

The Processor represents that, at the date of this DPA, it has no reason to believe that the laws and practices in any destination country applicable to the processing of Client Personal Data prevent it from fulfilling its obligations under this DPA. The Processor shall notify the Client promptly if it becomes aware of any such requirement.

Specific note on the executing entity: Where Justido LLC (United States) is the executing Processor and the Client or its Data Subjects are located in the EEA, the United Kingdom or Switzerland, the provision of the Services itself constitutes a Restricted Transfer, and the EU Transfer SCCs and (where applicable) UK IDTA in Annex IV apply directly between the Client and Justido LLC. Where Justido GmbH (Germany) is the executing Processor, transfers to Justido LLC or to other non-EEA Sub-Processors are governed by those same mechanisms, flowed down via Clause 4.3.

6. Audits and Inspections

The Processor shall make available to the Client all information necessary to demonstrate compliance with its obligations under Article 28 GDPR and this DPA, and shall allow for and contribute to audits, including inspections, conducted by the Client or another auditor mandated by the Client, subject to the following conditions:

- audits are limited to once per calendar year, unless triggered by a Personal Data Breach or a documented finding of non-compliance;
- the Client provides at least thirty (30) days' prior written notice, unless urgency reasonably requires shorter notice;
- audits are conducted during normal business hours, without unreasonable disruption to the Processor's operations, and subject to appropriate confidentiality undertakings;
- the Client bears the reasonable costs of audits it initiates, save where the audit reveals a material breach by the Processor, in which case the Processor bears the costs;
- the Processor may satisfy the Client's audit rights by providing recent third-party audit reports or certifications (such as SOC 2 Type II or ISO 27001), where these cover the relevant processing.

7. Liability, Term and Termination

The liability of each Party under this DPA is subject to the limitations and exclusions of liability set out in the Principal Agreement, except where such limitations are prohibited by Applicable Data Protection Laws.

This DPA takes effect on the effective date of the Principal Agreement and remains in force for as long as the Processor processes Client Personal Data on behalf of the Client. Provisions which by their nature survive termination (including confidentiality, liability and return/deletion obligations) shall continue to apply.

Either Party may terminate this DPA with immediate effect in the event of a material, uncured breach by the other Party of its obligations under Applicable Data Protection Laws or this DPA.

8. Governing Law and Miscellaneous

Where Justido GmbH is the executing Processor, this DPA is governed by the laws of the Federal Republic of Germany, excluding its conflict-of-laws rules and the UN Convention on Contracts for the International Sale of Goods. Exclusive place of jurisdiction shall be Berlin, Germany, to the extent legally permissible.

Where Justido LLC is the executing Processor, this DPA is governed by the laws of the State of Delaware, United States, excluding its conflict-of-laws rules. The Parties submit to the jurisdiction of the state and federal courts located in the State of Delaware, without prejudice to mandatory rights of Data Subjects under Applicable Data Protection Laws.

Notwithstanding the foregoing, the rights of Data Subjects under Applicable Data Protection Laws and, in particular, under the SCCs incorporated by reference in Annex IV, remain governed by the law applicable under those instruments.

If any provision of this DPA is held invalid or unenforceable, the remaining provisions continue in full force and effect, and the Parties shall replace the invalid provision with a valid one that most closely approximates the original economic and legal intent.

No variation to this DPA is valid unless made in writing and signed by authorised representatives of both Parties. Amendments to the Annexes may be made by written notice (including email) in accordance with the procedures set out in this DPA.

Signatures

The Parties, intending to be legally bound, have executed this Data Processing Agreement on the dates set out below.

For the Client (Controller):

Signature:

Name:

Title:

Place:

Date:

For the Processor — executing entity (tick one):

☐ *Justido GmbH*

Kurfürstendamm 37, 10719 Berlin, Germany
Amtsgericht Charlottenburg, HRB 250605 B
By: Stephan Hoffmann, Geschäftsführer

☐ Justido LLC
251 Little Falls Drive, Wilmington, Delaware 19808, USA
By:

Signature:

Name:

Title:

Place:

Date:

Annex I — Description of the Processing

Part A — List of Parties

Select the Processor entity that applies to this engagement. The default rule is: Justido GmbH acts as Processor for Clients established in the EEA, United Kingdom or Switzerland; Justido LLC acts as Processor for Clients established in the United States or other non-EEA jurisdictions. Either entity may, by mutual agreement, act as Processor for any Client.

Data Exporter / Controller

Legal name	
Registered address	
Registration number	
Contact person	

Role	Controller (or Processor on behalf of a Third-Party Controller)
Activities relevant to the data	Use of Justido's AI-enabled CRM, marketing automation, voice-agent and related services

Data Importer / Processor — Option 1 (default for EEA/UK/CH Clients)

Legal name	Justido GmbH
Registered address	Kurfürstendamm 37, 10719 Berlin, Germany
Commercial register	Amtsgericht Berlin (Charlottenburg), HRB 250605 B
VAT ID (USt-IdNr.)	DE285976038
Managing Director	Stephan Hoffmann, Peter Hoffmann
Privacy contact	privacy@justido.de
General contact	office@justidosolutions.com
Role	Processor

Data Importer / Processor — Option 2 (default for US / non-EEA Clients)

Legal name	Justido LLC
Registered address	251 Little Falls Drive, Wilmington, Delaware 19808, USA
State of formation	Delaware, United States
Privacy contact	privacy@justidosolutions.com
General contact	office@justidosolutions.com
Role	Processor

Entity executing this DPA (tick one):

☐ Justido GmbH

☐ Justido LLC

Part B — Description of the Transfer / Processing

Categories of Data Subjects	Client's end customers, leads, prospects, employees and authorised users; individuals who interact with Client's voice or chat agents, forms, pipelines or communications; individuals whose Personal Data is otherwise submitted to the Services by or on behalf of the Client.

Categories of Personal Data	Identifiers (name, email, phone); communication content (SMS, email, chat transcripts, call recordings, voicemail); voice data and voice-derived features (audio, transcripts, sentiment markers); CRM fields and pipeline data; appointment and scheduling data; marketing preferences and consent records; IP addresses and device/usage metadata; any additional categories submitted by the Client via the Services.
Special Categories of Data	None by default. The Client shall not submit (a) special categories of Personal Data within the meaning of Article 9 GDPR, (b) data relating to criminal convictions and offences within the meaning of Article 10 GDPR, (c) Protected Health Information ("PHI") within the meaning of the U.S. Health Insurance Portability and Accountability Act (45 CFR § 160.103), or (d) information falling within the definition of "Sensitive Personal Information" under any U.S. state privacy law, unless expressly agreed in writing, including additional safeguards and, where required, the execution of a separate Business Associate Agreement (in the case of PHI) or a Sensitive Personal Information addendum (in the case of state-law sensitive data).
Frequency of the Processing	Continuous, for the duration of the Principal Agreement.
Nature of the Processing	Configuration, deployment, operation, support and maintenance of AI-enabled CRM, marketing automation, voice-agent and related software services (including GoHighLevel, voice AI, generative-AI and hosting platforms) on behalf of the Client; collection, storage, organisation, analysis, transmission, disclosure to Sub-Processors, and deletion of Personal Data as required to provide the Services.
Purpose of the Processing	Provision of the Services agreed in the Principal Agreement, including CRM management, automated communications, lead qualification, appointment setting, voice-agent interactions, reporting and analytics.
Duration / Retention	Duration of the Principal Agreement plus the applicable return/deletion period set out in Clause 3.6, subject to legal retention obligations.
Transfers to Sub-Processors	Subject-matter, nature and duration of processing by Sub-Processors as set out in Annex III.

Part C — Competent Supervisory Authority

For processing falling within the territorial scope of the GDPR, the competent Supervisory Authority is the authority of the EU Member State in which the Client is established, or, where the Client is not established in the EU, the authority designated in accordance with Article 27 GDPR.

Where Justido GmbH is the executing Processor, the default competent Supervisory Authority is the Berliner Beauftragte für Datenschutz und Informationsfreiheit (Berlin Commissioner for Data Protection and Freedom of Information).

For processing subject to the UK GDPR, the competent authority is the Information Commissioner's Office (ICO). For Swiss data, the Federal Data Protection and Information Commissioner (FDPIC).

Annex II — Technical and Organisational Measures

The Processor implements and maintains the following technical and organisational measures (TOMs) to ensure a level of security appropriate to the risk, in accordance with Article 32 GDPR. These measures apply to Client Personal Data processed under this DPA, whether directly by the Processor or via its Sub-Processors.

1. Pseudonymisation and Encryption

- Encryption of Personal Data in transit using TLS 1.2 or higher for all external connections.
- Encryption of Personal Data at rest using AES-256 or equivalent industry-standard ciphers.
- Use of pseudonymisation where technically feasible and proportionate to the risk.

2. Confidentiality, Integrity, Availability

- Role-based access control applying the principle of least privilege.
- Multi-factor authentication required for all privileged access and for all access to systems processing Client Personal Data.
- Formal user provisioning and de-provisioning procedures; access reviewed at least every six (6) months.
- Local development environments are separated from production; deployments to production are gated through isolated preview branches on the underlying hosting platform.
- Written confidentiality obligations imposed on all personnel and contractors with access to Client Personal Data.

3. Availability and Disaster Recovery

- Regular, encrypted backups of Client Personal Data, stored redundantly across multiple availability zones, relying on the infrastructure of underlying certified cloud providers.
- Documented business continuity and disaster recovery plan, reviewed at least annually.
- Monitoring and alerting on the availability and integrity of systems processing Client Personal Data.

4. Testing, Assessment and Evaluation

- Automated dependency vulnerability scanning (Dependabot or equivalent) on all Processor-controlled code repositories, with review of moderate-severity-and-above findings within five (5) business days of disclosure.
- Reliance on the external penetration-testing and third-party audit programmes of underlying Sub-Processors (e.g., SOC 2 Type II reports from Retell AI, ElevenLabs, HighLevel, Vercel, Upstash, and Sentry) for infrastructure-level assurance.
- Documented information-security policies reviewed at least annually by management.
- Sub-Processor due-diligence and periodic re-assessment.

5. Data Minimisation and Quality

- Collection and processing of Client Personal Data limited to what is necessary for the Services.
- Mechanisms allowing the Client to correct, suppress or delete Client Personal Data on request or via self-service within the underlying platforms.

6. Accountability and Governance

- Maintenance of a Record of Processing Activities (Article 30 GDPR) covering processing carried out on behalf of clients.
- Designated privacy contact within the Processor (Stephan Hoffmann for Justido GmbH; Justido LLC contact via privacy@justidosolutions.com).
- Mandatory data protection and information-security training for all personnel with access to Personal Data, at onboarding and at least annually thereafter.
- Incident response plan with defined roles, escalation paths and notification procedures, including the 72-hour notification commitment under Clause 3.4.

7. Physical Security

- Client Personal Data is processed exclusively in certified data centres operated by reputable cloud providers (e.g., AWS, Google Cloud, Azure, Vercel, HighLevel infrastructure) with SOC 2 Type II or ISO 27001 certification or equivalent.
- The Processor operates remote-first and maintains no shared office locations. Personal computing devices used by Processor personnel to access Client Personal Data are subject to full-disk encryption, screen-lock enforcement and remote-wipe capability in the event of loss or theft.

8. Sub-Processor Measures

Where processing is carried out by a Sub-Processor, the Processor ensures that the Sub-Processor implements TOMs providing a level of protection equivalent to those described in this Annex, through contractually binding flow-down obligations, and relies on independent third-party certifications and audit reports of Sub-Processors where available.

Annex III — List of Approved Sub-Processors

The Processor engages the following Sub-Processors at the date of this DPA. The Processor shall update this list in accordance with Clause 4 of this DPA and notify the Client of any additions or replacements by email to the Client's designated contact at least ten (10) business days before the change takes effect.

Sub-Processor	Processing Location	Purpose / Service	Transfer Mechanism
Retell AI, Inc.	United States; EU region available	Voice-AI orchestration: agent runtime, in-browser web SDK (LiveKit-based WebRTC), tool-call webhook	EU 2021 SCCs (Module 2 / Module 3) + UK IDTA (incorporated in Retell DPA)

Sub-Processor	Processing Location	Purpose / Service	Transfer Mechanism
		routing, end-of-call event delivery. Anthropic (Claude LLM) and Deepgram (STT) are engaged by Retell as sub-sub-processors.	
ElevenLabs, Inc.	United States (EU data residency available on enterprise plans)	Text-to-speech synthesis (multilingual_v2 / turbo_v2_5 voice models); voice design for assistant voices.	EU 2021 SCCs + UK IDTA (incorporated in ElevenLabs DPA); EU-US Data Privacy Framework certified
HighLevel Inc. (GoHighLevel)	United States	CRM, pipelines, workflows, automations, SMS/email, client portals, booking calendars, contact storage.	EU 2021 SCCs + UK IDTA (incorporated in HighLevel DPA); EU-US Data Privacy Framework + UK Extension + Swiss-US DPF certified
Vercel, Inc.	United States; Global CDN edge	Hosting, edge functions, frontend application delivery for justidosolutions.com and the booking API.	EU 2021 SCCs + UK IDTA (incorporated in Vercel DPA)
Upstash, Inc.	United States; AWS multi-region (Upstash global edge)	Hosted Redis (key-value store) for rate-limit infrastructure: caps how many requests a single visitor IP can make to public API endpoints (audit form, voice-AI web demo token mint, voice-agent tool calls) within a sliding time window. Prevents bot abuse and outbound-call cost spikes. No call content, no form	EU 2021 SCCs (incorporated in Upstash Customer DPA); SOC 2 Type II.

Sub-Processor	Processing Location	Purpose / Service	Transfer Mechanism
		submission bodies, no audit-trail PII pass through Upstash.	
Functional Software, Inc. (Sentry)	United States (us-west-1)	Error tracking and performance monitoring across browser and server runtimes; surfaces application failures with stack traces and breadcrumbs.	EU 2021 SCCs (incorporated via Sentry MSA + DPA terms); EU-US Data Privacy Framework certified
Stripe, LLC (United States) / Stripe Payments Europe, Limited (Ireland; EU-account engagements)	United States; Ireland	Subscription billing for Justido customer engagements: card capture, charge processing, recurring subscription management, retry-on-failure, customer self-serve billing portal, tax handling. Tokenised — raw card data never touches Justido infrastructure.	EU 2021 SCCs Module 1 (C2C) + Module 2 (C2P) (incorporated in Stripe DPA at stripe.com/legal/dpa, last updated 18 November 2025); UK IDTA + Swiss adaptations; EU-US Data Privacy Framework + UK Extension + Swiss-US DPF (certified, Stripe, LLC); PCI DSS Level 1; SOC 1 + SOC 2.
Twilio Inc. (United States) / Twilio Ireland Limited (EU engagements where applicable)	United States; Ireland (EU region available for EU customer engagements)	SMS messaging, voice connectivity (PSTN call termination and origination), and phone-number provisioning for inbound and outbound calls in the AI-receptionist service. Engaged both directly by the Processor (Justido's own Twilio account) and indirectly as infrastructure within the HighLevel platform. Not used for email.	EU 2021 SCCs (Module 2 / Module 3) + UK IDTA (incorporated in Twilio Data Protection Addendum at https://www.twilio.com/legal/data-protection-addendum); EU-US Data Privacy Framework + UK Extension + Swiss-US DPF certified.

Sub-Processor	Processing Location	Purpose / Service	Transfer Mechanism
Justido LLC (Delaware, USA)	United States	Provision of the Justido Solutions technical stack as Sub-Processor of Justido GmbH where Justido GmbH is the contracting Processor under this DPA. Justido LLC holds the direct vendor agreements with the downstream sub-processors listed in this Annex; intra-group flow-down per the bilateral Intra-Group Data Processing Agreement between Justido LLC and Justido GmbH.	EU 2021 SCCs Module 3 (Processor-to-Processor) incorporated by reference in the Intra-Group DPA; Justido GmbH as data exporter, Justido LLC as data importer.
Anthropic, PBC	United States	AI assistant over Microsoft 365 — read-only access (Outlook mail, SharePoint, OneDrive, Teams, Calendar) via Anthropic's Microsoft 365 connector; lets Claude search, read and summarise the Processor's M365 content to support its personnel. No send / edit / delete. Operates under Anthropic's commercial zero-retention / no-training terms (Clause 3.7). Separate from Anthropic's sub-sub-	EU 2021 SCCs under Anthropic's commercial DPA; UK IDTA where applicable; EU-US Data Privacy Framework where Anthropic is certified.

Sub-Processor	Processing Location	Purpose / Service	Transfer Mechanism
		processor role via Retell AI — this is the direct engagement.	
Microsoft Ireland Operations Limited	European Union — tenant region Germany (Microsoft EU Data Boundary)	Business email, calendar, document storage and collaboration (Exchange Online, SharePoint, OneDrive, Teams) for the Processor; may contain Client Personal Data appearing in business correspondence and documents. Hosts the Microsoft 365 environment the Anthropic connector reads.	Processing within the EU/EEA (EU Data Boundary); Microsoft Product Terms + DPA, with EU 2021 SCCs for any onward / support transfers outside the EEA.

Each of the Sub-Processors listed above operates under its own Data Processing Agreement with the Processor, incorporating the EU 2021 SCCs and (where applicable) the UK IDTA. The Processor has executed or accepted those DPAs in respect of both Justido GmbH and Justido LLC, as applicable.

Annex IV — International Data Transfer Mechanisms

This Annex sets out the transfer mechanisms that apply to Restricted Transfers under this DPA. The specifications in this Annex supplement the incorporation by reference set out in Clause 5.

1. EU Transfer SCCs (Commission Implementing Decision (EU) 2021/914)

The EU Transfer SCCs are incorporated by reference into this DPA. The Parties agree the following options and specifications:

- Applicable Module: Module 2 (Controller-to-Processor) where the Client acts as Controller; Module 3 (Processor-to-Processor) where the Client acts as Processor on behalf of a third-party controller.
- Clause 7 (Docking Clause): does not apply.
- Clause 9 (Use of Sub-Processors): Option 2 — general written authorisation; the time period for prior notice of Sub-Processor changes is ten (10) business days (see Clause 4.2 of this DPA).
- Clause 11 (Redress): the optional language does not apply.

- Clause 17 (Governing Law): the SCCs are governed by the law of Ireland where the Client is established in the EEA, or, where the Client is established in Germany, by the law of the Federal Republic of Germany.
- Clause 18 (Choice of Forum and Jurisdiction): disputes arising from the SCCs shall be resolved by the courts of Ireland, or, where German law is chosen under Clause 17, by the courts of Berlin, Germany.
- Annex I.A (List of Parties): as set out in Annex I, Part A of this DPA.
- Annex I.B (Description of Transfer): as set out in Annex I, Part B of this DPA.
- Annex I.C (Competent Supervisory Authority): as set out in Annex I, Part C of this DPA.
- Annex II (Technical and Organisational Measures): as set out in Annex II of this DPA.
- Annex III (List of Sub-Processors): as set out in Annex III of this DPA.

2. UK International Data Transfer Addendum (UK IDTA)

Where Personal Data is transferred from the United Kingdom and such transfer is subject to the UK GDPR, the UK IDTA (version B1.0, issued by the UK Information Commissioner under section 119A of the UK Data Protection Act 2018, in force since 21 March 2022) is incorporated by reference. The Parties agree the following:

- Table 1 (Parties): as set out in Annex I, Part A of this DPA.
- Table 2 (Selected SCCs, Modules and Clauses): the EU Transfer SCCs as specified in Section 1 of this Annex IV.
- Table 3 (Appendix Information): as set out in Annex I, Part B, Annex II and Annex III of this DPA.
- Table 4 (Ending the Addendum when the Approved Addendum changes): either Party may end the UK IDTA.

3. Swiss Transfers

Where Personal Data is transferred from Switzerland and such transfer is subject to the Swiss FADP, the EU Transfer SCCs apply with the following adaptations, consistent with the guidance of the Swiss Federal Data Protection and Information Commissioner:

- references to the GDPR are to be interpreted as references to the FADP where transfers are governed exclusively by Swiss law;
- the competent Supervisory Authority is the Swiss Federal Data Protection and Information Commissioner;
- the term “Member State” is read so as not to exclude data subjects in Switzerland from exercising their rights in their place of habitual residence.

4. Where Justido LLC is the Importer

Where Justido LLC is the executing Processor under this DPA and Personal Data is transferred from the EEA, United Kingdom or Switzerland to Justido LLC in the United States, the EU Transfer SCCs and (where applicable) the UK IDTA and Swiss adaptations in this Annex IV apply directly between the Client (as Exporter) and Justido LLC (as Importer), and are deemed signed by both Parties upon execution of this DPA.

Where Justido GmbH is the executing Processor and it transfers Personal Data onward to Justido LLC or to any other Sub-Processor located outside the EEA, those onward transfers are covered by the corresponding DPA and SCCs between Justido GmbH and the onward recipient, and the Processor remains fully liable to the Client for such onward transfers in accordance with Clause 4.3.

Annex V — U.S. State Privacy Addendum

This Annex applies to Personal Information of natural persons resident in the United States that is processed by the Processor on behalf of the Client under the Principal Agreement and is subject to one or more of the U.S. state privacy laws listed in Section 12 below (collectively, "U.S. State Privacy Laws"). Capitalised terms used in this Annex and not defined here have the meanings given to them in the applicable U.S. State Privacy Law; where definitions differ across laws, the California Consumer Privacy Act / California Privacy Rights Act ("CCPA/CPRA") definitions apply.

1. Roles. With respect to Personal Information of U.S. residents processed under the Principal Agreement, the Client is the "Business" (or "Controller" where applicable) and the Processor acts as a "Service Provider" (or "Processor"/"Contractor"/"Third Party" as required by the applicable U.S. State Privacy Law).

2. Limited Purpose. The Processor shall process Personal Information only for the Business Purpose(s) set out in the Principal Agreement and Annex I of this DPA, and shall not retain, use or disclose Personal Information for any purpose other than (a) the specific Business Purpose(s) of providing the Services, (b) as otherwise permitted by the CCPA/CPRA and applicable U.S. State Privacy Laws, or (c) as required by law.

3. No Sale, No Sharing. The Processor shall not "sell" or "share" Personal Information within the meaning of the CCPA/CPRA, and shall not engage in "Targeted Advertising" or process Personal Information for "Cross-Context Behavioral Advertising" or "Profiling in furtherance of decisions that produce legal or similarly significant effects" within the meaning of any applicable U.S. State Privacy Law.

4. No Combination Outside Business Purpose. The Processor shall not combine Personal Information received from or on behalf of the Client with Personal Information received from or on behalf of any third party, or collected from its own interactions with the individual, except as expressly permitted by the CCPA/CPRA and applicable U.S. State Privacy Laws to perform the Business Purpose.

5. Compliance Certification. The Processor certifies that it understands the restrictions in Sections 2–4 of this Annex and will comply with them.

6. Notice of Inability to Meet Obligations. The Processor shall promptly notify the Client if it makes a determination that it can no longer meet its obligations under the CCPA/CPRA or any applicable U.S. State Privacy Law. Upon such notice, the Client may take reasonable and appropriate steps to stop and remediate unauthorised use of Personal Information.

7. Consumer Rights Assistance. The Processor shall assist the Client, taking into account the nature of the processing, in responding to verifiable consumer requests received by the Client under U.S. State Privacy Laws, including requests to know, access, correct, delete, port and opt out of sale/sharing/targeted advertising. The Processor shall pass through any Universal Opt-Out Mechanism (such as the Global Privacy Control) signals it receives, where technically feasible.

8. Sensitive Personal Information. The Processor shall treat any Personal Information designated as "Sensitive Personal Information" under the CCPA/CPRA or "Sensitive Data" under other U.S. State Privacy Laws in accordance with the applicable law's heightened requirements, including any consent or purpose-limitation requirements. The Client shall not submit Sensitive Personal Information to the Processor unless agreed in writing pursuant to Annex I, Part B.

9. Sub-Processor Flow-Down. The Processor shall ensure that each Sub-Processor engaged to process Personal Information of U.S. residents is bound by written terms imposing data-protection obligations substantially equivalent to those set out in this Annex, including the restrictions in Sections 2–4 above.

10. Deletion. Upon the Client's verifiable consumer-deletion request forwarded to the Processor under Section 7, the Processor shall delete the relevant Personal Information from its systems within thirty (30) days, subject to the exceptions permitted under the applicable U.S. State Privacy Law (e.g., to comply with a legal obligation, to detect security incidents, or to defend legal claims).

11. Audit. The Client may, no more than once per calendar year and subject to the audit conditions set out in Clause 6 of the body of this DPA, take reasonable and appropriate steps to ensure the Processor uses Personal Information in a manner consistent with the Client's obligations under U.S. State Privacy Laws.
12. Covered Laws. This Annex applies to processing of Personal Information subject to the following U.S. state privacy laws, each as amended from time to time: California Consumer Privacy Act / California Privacy Rights Act (CCPA/CPRA); Virginia Consumer Data Protection Act (VCDPA); Colorado Privacy Act (CPA); Connecticut Data Privacy Act (CTDPA); Utah Consumer Privacy Act (UCPA); Texas Data Privacy and Security Act (TDPSA); Oregon Consumer Privacy Act (OCPA); Montana Consumer Data Privacy Act (MTCDPA); Florida Digital Bill of Rights (FDBR); Delaware Personal Data Privacy Act (DPDPA); Indiana Consumer Data Protection Act (INCDPA); Kentucky Consumer Data Protection Act (KCDPA); Minnesota Consumer Data Privacy Act (MCDPA); New Jersey Data Privacy Act (NJDPA); Tennessee Information Protection Act (TIPA); and any further U.S. state, federal or territorial privacy law that comes into force during the term of the Principal Agreement, to the extent applicable.
In the event of a conflict between this Annex V and the body of the DPA or any other Annex, this Annex V prevails with respect to the processing of Personal Information of U.S. residents subject to U.S. State Privacy Laws.

Disclaimer

This Data Processing Agreement is maintained by Justido GmbH and Justido LLC as the standard processor template for their respective client engagements. Annex I, Part A must be completed before signing.

— End of Data Processing Agreement —