Data Processing Agreement — Jithox

Standard Contractual Clauses between controllers and processors, Commission Implementing Decision (EU) 2021/915 of 4 June 2021, Article 28(7) GDPR. Source text: https://eur-lex.europa.eu/eli/dec_impl/2021/915/oj (Official Journal L 199, 7.6.2021, p. 18).

Based on the EU SCC 2021/915; not legal advice. Sections I to III are the Commission's text, copied word for word. Only the options and the Annexes are filled in by Jithox.

Signed on request: mail info.jithox@gmail.com.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights

or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 - Optional

Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II — OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7

Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor’s opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to

ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to

sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 of Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III — FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I — List of parties

Controller(s):

1. Name: the customer of Jithox that accepts these Clauses (the business that uses a Jithox service for its own customers, suppliers or staff).
   Address: as stated by the customer when accepting.
   Contact person's name, position and contact details: as stated by the customer when accepting.
   Signature and accession date: on acceptance, or on a signed copy on request.

Processor(s):

1. Name: Victor-Emmanuel Charlier, trading as Jithox (sole trader, natural person). KBO/BCE 1039.898.594, VAT BE1039898594.
   Address: available on request via info.jithox@gmail.com.
   Contact person's name, position and contact details: Victor-Emmanuel Charlier, owner, info.jithox@gmail.com. No data protection officer has been appointed.
   Signature and accession date: on request (see "Signed on request" above).

ANNEX II — Description of the processing

This Annex covers three Jithox services. A customer only uses the rows of the service(s) it actually uses.

A. Jithox MCP and HTTP checks (EU e-invoicing and company checks for software and AI agents). B. Invoice

Status (reading sales-invoice status from the customer's own Moneybird administration). C. Jithox for WhatsApp / workspace (preparing quotes, invoices and customer answers from messages).

Categories of data subjects whose personal data is processed

- A: sole traders and other natural persons whose VAT number, company number or Peppol participant id the controller submits in a call, persons named in an invoice document the controller submits, and persons named in or heard on a receipt image or audio file the controller submits to the MCP tools parse_receipt_vision and transcribe_and_slice_audio.
- B: the controller's invoice counterparties, as far as a returned company name, invoice identifier, date or amount relates to a natural person.
- C: the controller's own customers and contacts who send messages or appear in quotes and invoices; the controller's own staff who sign in and approve.

Categories of personal data processed

- A: VAT numbers, company numbers, Peppol participant ids, and the content of invoice documents submitted for a check (names, addresses, IBAN, amounts, as present in the document); images of receipts and audio files the controller submits to the MCP tools parse_receipt_vision and transcribe_and_slice_audio, and the text extracted from them.
- B: Moneybird administration id and name, invoice number, invoice dates, amounts and company names. Jithox removes free reference text and contact first name, last name, e-mail, phone and address before returning a result.
- C: messages the controller pastes or forwards, and the quotes, invoices, drafts and questions prepared from them; the controller's own business details (name, VAT number, address, IBAN); customer details the controller explicitly saves; approvals and receipts (who approved what, when, and what the provider confirmed).
- All services: sign-in identity of the controller's users (e-mail address, name) via the sign-in provider; per accepted call a usage count and a signed receipt.

Sensitive data processed (if applicable) and applied restrictions or safeguards

None intended. The services are not designed for the special categories of Article 9 GDPR or for data relating to criminal convictions. If the controller nevertheless submits such data in a message or document, it is processed only to answer that call and the Annex III measures apply. No additional safeguard specific to sensitive data exists today.

Nature of the processing

- A: receiving the submitted identifiers or document, querying public EU sources (for example the European Commission's VIES service for VAT numbers), and returning a typed answer with a signed receipt; for parse_receipt_vision and transcribe_and_slice_audio, sending the submitted image or audio to OpenAI (Annex IV) to read or transcribe it. Without an OpenAI key configured these tools refuse the call. Whether production has that key: ONBEKEND, eigenaar controleren.
- B: sending the administration id and filters, or the invoice number, to Moneybird with the controller's own encrypted, account-bound Moneybird permission; returning selected fields. No AI model is invoked. Jithox does not durably store the query or the result; administration ids and names are cached in process for 60 seconds.
- C: storing messages and business details in the controller's workspace, preparing drafts (optionally with an AI model, see Annex IV), and executing an outbound action (e-mail, invoice, message) only after a person approves the exact content.

Purpose(s) for which the personal data is processed on behalf of the controller

Only to deliver the check, status read or prepared document the controller requested, and to keep the usage count, balance and receipt trail for that request. No selling of data and no advertising.

Duration of the processing

- For the duration of the contract, and after that until deletion under Clause 10(d).
- Invoice Status results: not durably stored; in-process cache entries are reused for 60 seconds.
- WhatsApp messages received: the workspace holds the twenty most recent and nothing older.
- Quotes, invoices, approvals and receipts: kept, because they are the controller's accounting and authorisation trail. There is no automatic purge; deletion is carried out by a person on request.
- Closed account: the e-mail address is overwritten with a placeholder and the display name and picture are cleared; the emptied record stays because receipts refer to it.

For processing by (sub-)processors, also specify subject matter, nature and duration of the processing

See Annex IV.

Not covered by this Annex: the aggregated visit measurement on Jithox's own public website. For that, Jithox decides the purpose and means itself; it is described on /privacy.

ANNEX III — Technical and organisational measures including technical and organisational measures to ensure the security of the data

Jithox holds no certification (no SOC 2, ISO 27001, HIPAA or PCI) and has had no independent penetration test.

- Protection of data during transmission. The site and API are served over HTTPS only; the response header Strict-Transport-Security: max-age=63072000; includeSubDomains pins HTTPS.
- Location of processing. Application compute runs in Vercel region fra1 (Frankfurt). The database is Neon Postgres in eu-central-1 (Frankfurt).
- Protection of data during storage, encryption. Third-party credentials that a controller connects (for example a Moneybird permission, WhatsApp connection tokens) are encrypted with AES-256-GCM before storage; the service refuses to store them unencrypted if the key is missing.
- Pseudonymisation / hashing. API keys are stored only as a SHA-256 hash, never in raw form.
- Separation between customers. Tenant tables use Postgres row-level security with FORCE ROW LEVEL SECURITY, so the isolation policy also applies to the table owner.
- User identification and authorisation. Sign-in runs through Clerk; OAuth scopes and hashed API keys authorise machine calls.
- Accountability and event logging. Every side-effecting action requires an explicit human approval bound to the exact content, is executed at most once (idempotency key claimed before the provider is called), and produces an append-only receipt signed with Ed25519 that the controller can verify independently.
- Data minimisation. Invoice Status strips contact names, e-mail, phone, address and free reference text before returning a result; card data never reaches Jithox (Stripe hosted checkout).
- Limited data retention. See Annex II, Duration. There is no automated deletion pipeline; a person carries out deletion requests.
- Erasure and portability. Deletion is handled per request type as described on /data-deletion. A portability export is not built; data is provided by hand on request.
- Personnel. Jithox is one natural person trading alone; access to production data is limited to that person.
- Assistance to the controller (Clauses 8 and 9). Requests and breach notifications go to info.jithox@gmail.com. A breach notification under Clause 9.2 is sent to the contact address the controller gave in Annex I.
- Not in place (stated so the controller can assess): no uptime figure or SLA, no audited backup or restore

procedure documented by Jithox, no independent security test, no data protection officer.

ANNEX IV — List of sub-processors

The controller authorises the following sub-processors (Clause 7.7(a), general written authorisation, 14 days' advance notice of a new sub-processor via the /dpa page — see the filled-in options above). Every service listed is one the code can call; the "Engaged" column states whether that happens for every controller or only when a named feature is switched on for that controller, so "engaged when named feature is active" is not a gap in the list, it is a true description of when Jithox actually sends data to that sub-processor.

1. **Vercel Inc.**
   What it does for Jithox: Hosting of the website, API and app
   Engaged: Always
   Where (as published by the sub-processor): Region fra1 (Frankfurt), configured and measured
   Its own DPA / sub-processor list: https://vercel.com/legal/dpa
   Source in code: vercel.json:8

2. **Neon**
   What it does for Jithox: Postgres database for all application data
   Engaged: Always
   Where (as published by the sub-processor): eu-central-1 (Frankfurt)
   Its own DPA / sub-processor list: https://neon.com/dpa (redirects to platform terms §3.4)
   Source in code: src/lib/db.ts:110-111

3. **Hetzner Online GmbH**
   What it does for Jithox: Servers of the MCP fleet on mcp.jithox.com
   Engaged: Always
   Where (as published by the sub-processor): Helsinki, Finland (measured: AS24940)
   Its own DPA / sub-processor list: https://www.hetzner.com/AV/DPA_en.pdf
   Source in code: docs/website/ZAKELIJK_AFNEMEN.md:24

4. **Clerk, Inc.**
   What it does for Jithox: Sign-in: e-mail, name, session
   Engaged: Always
   Where (as published by the sub-processor): United States, per Clerk's own DPA (account data is processed under the EU-U.S. Data Privacy Framework; Clerk's Trust Center sub-processor list is at clerk.com/legal/subprocessors, current as of 10-07-2026)
   Its own DPA / sub-processor list: https://clerk.com/legal/dpa
   Source in code: package.json (@clerk/nextjs); src/features/auth/clerk.ts

5. **Stripe**
   What it does for Jithox: Card payment and checkout: buyer name, e-mail, billing address, VAT id
   Engaged: Always (paid orders)
   Where (as published by the sub-processor): Ireland (Stripe Payments Europe, Ltd., contracting entity for a non-US account) and United States (Stripe, Inc., operational replication for fraud prevention), per Stripe's own DPA §1 and §3.2
   Its own DPA / sub-processor list: https://stripe.com/legal/dpa
   Source in code: package.json (stripe)

6. **Resend**
   What it does for Jithox: Sending e-mail and receiving inbound e-mail (addresses, message content)
   Engaged: Always
   Where (as published by the sub-processor): United States, per Resend's own sub-processor list (resend.com/legal/subprocessors); Resend's DPA (§4) names the list as authoritative
   Its own DPA / sub-processor list: https://resend.com/legal/dpa

Source in code: src/features/mcp-email/client/email-client.ts:215; src/features/workspace/inbound-email-body.ts:21

7. OpenAI

What it does for Jithox: A (MCP tools parse_receipt_vision, transcribe_and_slice_audio: receipt images and audio files) and C (drafting, receipt reading, audio transcription)
Engaged: Only if OPENAI_API_KEY is set for the controller's account; the tools refuse the call otherwise
Where (as published by the sub-processor): Mixed, per OpenAI's published sub-processor list for the API product (platform.openai.com/subprocessors, checked 23-09-2026): Microsoft (cloud infrastructure) is listed for 22 countries including several EU/EEA states (e.g. France, Germany, Ireland, Italy, Netherlands, Poland, Spain, Sweden), CoreWeave lists Sweden among its countries, Google Cloud Platform lists Finland and Netherlands, while Amazon Web Services is listed as United States only; the list does not state which entity or country handles a given request
Its own DPA / sub-processor list: ONBEKEND whether Jithox has a signed DPA with OpenAI on file (the provider's own DPA page returned HTTP 403 to our automated check on 23-09-2026); the platform.openai.com/subprocessors page above is public and does not require sign-in
Source in code: src/features/hosted-draft-beta/hosted-openai-draft-transport.ts:25; src/features/mcp-plugins/plugins/receipt-vision-plugin.ts:189; src/features/mcp-plugins/plugins/transcribe-audio-plugin.ts:162

8. Anthropic

What it does for Jithox: Only in C: drafting with a model key the customer brings
Engaged: Only when the controller configures an Anthropic model key
Where (as published by the sub-processor): Worldwide, per Anthropic's own sub-processor list (trust.anthropic.com/subprocessors, checked 23-09-2026: AWS and Google Cloud, the underlying infrastructure for all products, are both listed with country "Worldwide", not a specific country)
Its own DPA / sub-processor list: https://www.anthropic.com/legal/data-processing-addendum
Source in code: src/features/model-engine/model-engine.ts:67

9. DeepSeek

What it does for Jithox: Only in C: fallback model for drafting
Engaged: Only if the DeepSeek fallback is configured (owner does not use it today, see PRODUCT memory)
Where (as published by the sub-processor): People's Republic of China, as stated in DeepSeek's own privacy policy (cdn.deepseek.com/policies/en-US/deepseek-privacy-policy.html, "Data storage": "we directly collect, process and store your Personal Data in People's Republic of China")
Its own DPA / sub-processor list: ONBEKEND — DeepSeek publishes a privacy policy, not a GDPR-standard DPA or SCC package; no EU adequacy decision covers China
Source in code: src/features/ai-gateway/config.ts:47; src/features/ai/deepseek.ts:25

10. Upstash (Redis)

What it does for Jithox: Rate limiting and duplicate detection
Engaged: Only if configured (Upstash env vars set for the deployment)
Where (as published by the sub-processor): Selectable AWS region at database-creation time (Upstash documents both EU options, e.g. eu-west-1 Ireland and eu-central-1 Frankfurt, and US options); which region the current database uses is ONBEKEND, eigenaar controleren
Its own DPA / sub-processor list: https://upstash.com/static/trust/dpa.pdf (sub-processor list at upstash.com/static/trust/subprocessors.pdf)
Source in code: src/features/security/rate-limit-store.ts:149-150; src/features/agent-preflight/dedupe-store.ts:62-63

11. Vercel Blob

What it does for Jithox: Storage of media files
Engaged: Only if used (a controller submits a receipt image/audio file or other stored media)
Where (as published by the sub-processor): Covered by the Vercel DPA and the Vercel region configured for the project (see row 1: fra1, Frankfurt); Vercel Blob does not publish a separate region list from the main platform

Its own DPA / sub-processor list: https://vercel.com/legal/dpa
Source in code: src/features/media-assets/store.ts:34

12. Google Cloud Tasks

What it does for Jithox: Queue for agent actions
Engaged: Only if enabled (the owner does not use this today)
Where (as published by the sub-processor): Region is a per-project GCP configuration choice; Google's Cloud DPA (cloud.google.com/terms/data-processing-addendum §10) states data may be processed in any country where Google or its sub-processors maintain facilities unless a region is pinned; which region Jithox would pin is ONBEKEND, eigenaar controleren (not configured)
Its own DPA / sub-processor list: https://cloud.google.com/terms/data-processing-addendum
Source in code: src/features/agent-actions/google-cloud-tasks-agent-action-dispatch-queue.ts:247

13. Sentry

What it does for Jithox: Error monitoring
Engaged: Only if SENTRY_DSN is set
Where (as published by the sub-processor): Depends on the data-storage-location setting a Sentry customer picks at signup (EU or US region); Sentry's own sub-processor list (sentry.io/legal/subprocessors) names AWS, Google Cloud and Cloudflare as its infrastructure, each available in EU or US; which region Jithox's project uses is ONBEKEND, eigenaar controleren (not configured)
Its own DPA / sub-processor list: https://sentry.io/legal/dpa/
Source in code: src/features/monitoring/error-monitoring.ts:66-67

14. Telegram

What it does for Jithox: Notification that a draft is ready
Engaged: Only if configured (the owner does not use this today)
Where (as published by the sub-processor): For EEA/UK sign-ups Telegram states its data centres are in the Netherlands (telegram.org/privacy §"Where do we store your data"); a bot's outbound message to an existing chat runs over the same Telegram infrastructure
Its own DPA / sub-processor list: https://telegram.org/privacy (no separate GDPR sub-processor DPA is published for the Bot API; the Standard Bot Privacy Policy at telegram.org/privacy-tpa applies to bots without their own policy)
Source in code: src/features/workspace/draft-ready-notifier.ts:83

15. Payhip

What it does for Jithox: Sale and delivery of Jithox downloads (withdrawn from sale on 2026-09-18; existing buyers keep access); sends Jithox a webhook with buyer data, of which Jithox stores the buyer e-mail only as a SHA-256 hash
Engaged: Only for existing buyers of the withdrawn product; no new sales
Where (as published by the sub-processor): EU, per Payhip's own privacy policy (payhip.com/privacy, "Where we store your personal data": "All information We hold about you is stored on secure servers in the EU"); the data controller, Payhip Limited, is registered in London, UK, but that is the controller's registered office, not the stated storage location
Its own DPA / sub-processor list: ONBEKEND — Payhip publishes a privacy policy, not a standalone GDPR DPA; no separate sub-processor list found
Source in code: src/content/site/offers.ts:158-159,166; src/app/api/webhooks/payhip/route.ts:69

Services the controller connects with its own account (Moneybird for Invoice Status, Meta WhatsApp Business, Twilio, Mollie, Notion, Google Calendar, Google Sheets, X/Twitter) are the controller's own providers: Jithox acts on them with the controller's permission, under the controller's own contract with that provider, only when the controller connects that provider — this is not a Jithox sub-processor relationship because Jithox is not the controller's counterparty for that processing. Whether each of these is in fact the controller's own account and not a Jithox account is enforced by the connection flow (the controller authorises via that provider's own OAuth or API-key screen); Jithox does not hold a shared account with any of these providers on the controller's behalf.

Public registers queried for a check are recipients of the submitted identifier, not sub-processors: the European Commission's VIES service, the Belgian KBO/BCE (kbopub.economie.fgov.be), the Dutch KvK (api.kvk.nl) and UK Companies House (api.company-information.service.gov.uk; the United Kingdom is a third country with an EU adequacy decision).