Translation provided for convenience. The French version is the only legally binding one.

GDPR data processing agreement

Data processing agreement (Article 28 of the GDPR). Version of October 4, 2026.

Parties

The Client: _____, company registration (SIREN) _____, registered office _____, represented by _____, _____.

This agreement binds the Customer, meaning the organization that uses Please Send It in a professional capacity (company, association, self-employed person), as controller, and PAPEL SAS, a company with share capital of €100, Paris Trade and Companies Register 843 729 864, 58 rue de Monceau, 75008 Paris, which publishes the service, as processor. It forms part of the Terms of Use: it is accepted with them, when the account is created, and applies as soon as the service is used in a professional capacity; the accepted version, the date and the account that accepted it are recorded. From "My organization", the Customer can also download this agreement as a PDF, with its annexes and its organization's identity, then accept it online or sign it electronically on behalf of its organization; the accepted or signed copy is kept there.

1. Purpose

On the Customer's behalf and instructions, PAPEL hosts, delivers and makes available to it the documents, links, answers and signatures its contributors upload, and sends invitations, reminders and thank-you messages on its behalf through the channels the Customer chooses for each campaign: email, text message, call with a synthetic voice, call by a voice agent, letter, registered letter with acknowledgement of receipt, postcard.

Depending on the options the Customer uses, PAPEL also carries out on its behalf: electronic signature of documents; AI review of the documents received; checking that an uploaded link is accessible (PAPEL's server opens the address itself, with no provider); the summary and written transcript of calls by an agent; the transcription of the "Tell me in a voice note" recording and the suggestion of campaign scenarios; keeping the "My contributors" contacts; copying the documents received to the online storage the Customer has connected. The terms "campaign", "request" and "sequence" have the meaning given in section 1 of the Terms of Use.

2. Data and data subjects

- Data subjects: the contributors designated by the Customer, and the members of the Customer's organization.

- Data: name, email, phone number, postal address; uploaded files, which may contain ID documents, bank details, pay slips, videos; links and written answers; date of last visit; electronic signatures and their certificate of completion; delivery status of messages and calls; summary and written transcript of calls by an agent.

- Health data: Please Send It is not a certified health data host. The Customer does not use it to collect health data produced in the course of prevention, diagnosis or care (medical record, report, prescription). If the Customer asks a question or requests a document that reveals health information (an allergy or diet for a meal, a medical certificate of fitness for sport, proof of vaccination), this is a special category of data within the meaning of Article 9 of the GDPR: the

Customer, as controller, makes sure it can rely on one of the exceptions provided by that article (in practice, the person's explicit consent, or a legal or regulatory obligation authorizing it to ask), makes the question optional when nothing requires it, asks only for what is strictly necessary, and chooses the shortest retention period (30 days after the deadline).

3. Term and retention

The agreement lasts as long as the Customer's account. The Customer sets, for each campaign (and by default for its organization), how long the files received are kept: "as short as possible" (default setting: sensitive documents deleted 30 days after they arrive, other files at the end of the campaign), "until the end of the campaign" (all files, sensitive documents included, until that date), or "legal period for my profession" (all files until 5 years after the deadline, on a justification written by the Customer and recorded in the campaign log). It can also mark a document "keep": its files are kept 5 years after the deadline. The campaign ends from 30 days to one year after the deadline, by default 90 days after; upload links are then closed. Each file is deleted automatically when its period expires, and the Customer is notified by email 7 days before. The Customer alone is responsible for the period it chooses and its justification, in particular when its obligation runs longer (for example 5 years after the end of a business relationship that continues after the campaign, article L561-12 of the French Monetary and Financial Code): it must then archive these documents before they are deleted. The Customer can delete a campaign and its files at any time.

The log of each campaign (events timestamped to the second, the person acting, names, sizes and SHA-256 fingerprints of the files, without the files themselves) is kept 5 years after the campaign closes or is deleted, then deleted; it is deleted with the Customer's organization.

The "My contributors" contacts (names, contact details, sending preferences, groups, the Customer's free note, history of campaigns) are kept on the Customer's instructions, filled by their entries, their file imports and, if they leave it on, their launched campaigns. A contact unused for 3 years is deleted automatically; the Customer can delete a contact at any time. When a person asks not to be contacted any more from their upload page, their contact is blocked for the Customer and the service sends them no further message; the blocked contact is kept as long as the account exists, to enforce that request.

4. Instructions

PAPEL processes the data only on the Customer's documented instructions: the settings of its campaigns and its actions in the interface or through the API. PAPEL informs the Customer if an instruction appears to it to infringe the GDPR.

5. Confidentiality

The persons authorized to process the data at PAPEL are bound by a duty of confidentiality and only access the documents for a technical operation requested by the Customer or a legal obligation.

6. Security

See Annex 1: security measures.

7. Sub-processors

The Customer authorizes the following sub-processors:

See Annex 2: sub-processors and places of processing.

Stripe processes the Customer's own payments, as PAPEL's provider; it receives no contributor data. Any addition or replacement of a sub-processor, including a change of AI provider, is announced to the Customer by email 30 days in advance; the Customer can object by terminating free of charge.

In accordance with Article 28(4) of the GDPR, PAPEL imposes on each sub-processor, by contract, the same data protection obligations as those set out in this agreement, in particular sufficient guarantees regarding technical and organizational measures. Where a sub-processor fails to fulfil its obligations, PAPEL remains fully liable to the Customer for their performance.

8. Assistance

PAPEL helps the Customer respond to requests to exercise data subjects' rights: any request received directly is forwarded to the Customer within 5 business days. PAPEL also helps the Customer, on request, with its impact assessments and its exchanges with the CNIL. Each message sent to contributors states the Customer's name and includes a link to stop receiving reminders; the Customer is notified when a contributor uses it.

9. Personal data breach

PAPEL notifies the Customer of any personal data breach as soon as possible, and no later than 48 hours after discovering it, so that the Customer can, where applicable, notify the CNIL within 72 hours (Article 33 of the GDPR). The notification describes at least, to the extent these elements are known:

- the nature of the breach, including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of records concerned;

- the name and contact details of the contact person at PAPEL from whom more information can be obtained;

- the likely consequences of the breach;

- the measures taken or proposed to address it and to mitigate its consequences.

What is not yet known is provided afterwards, in phases, without undue delay. PAPEL documents each breach and gives the Customer the assistance needed to inform, where applicable, the data subjects.

10. End of the agreement

At the end of the agreement, PAPEL deletes all data and copies within 30 days, unless a legal retention obligation applies. Before that, the Customer can export everything: one ZIP per campaign, with its log and the file manifest.

11. Audit

PAPEL makes available to the Customer the documentation demonstrating compliance with this agreement. The Customer may have an audit carried out at most once a year, at its own expense, with 30 days' notice.

12. Transfers

By default, the service, its database, the files received and their backups are hosted and processed in the European Union, in France (Hostinger, Scaleway), and emails, text messages and postal sends go through French providers (Brevo, Merci Facteur). Without the options below, no contributor data is transferred outside the European Union.

Only the options the Customer chooses to use involve processing outside the European Union, in the United States, and only for the data described in section 7:

- a "Call" step: Twilio;

- a "Call by an agent" step: ElevenLabs, Google for the Gemini language model, and Twilio for routing the call;

- AI document review, and the scenario suggestions of "Tell me in a voice note": Anthropic.

These transfers are covered by the standard contractual clauses adopted by the European Commission (Article 46 of the GDPR), entered into with each provider or included in its data processing terms.

Annex 1: technical and organisational security measures

- Encrypted connection (HTTPS) and strict security headers; no resources loaded from another site on contributors' upload pages (on other pages, only the cookieless Umami audience measurement script is loaded, from a server administered by PAPEL).

- Files received encrypted at rest (AES-256-GCM), each with its own key, protected by a master key kept outside the data and the backups.

- Files received stored at Scaleway in Paris, encrypted before sending; continuous and hourly backup of the database, encrypted too; former versions and backups kept 30 days at the most.

- Files isolated by campaign and by contributor, content of each file checked on arrival, personal and secret upload links.

- Passwords, API keys and security links stored as hashes; API keys revocable and rate-limited.

- Log of the organization's sensitive actions (invitations, roles, deletions, keys, automatic deletions).

- Log of each campaign, exportable as CSV and included in the ZIP with the file manifest (SHA-256 fingerprint of each file received); PDF upload receipt for each contributor.

- Two-factor authentication (one-time code given by an authenticator app, with backup codes), which each password user can turn on and which the Customer can require for the members of its organization; the Customer can also restrict access to its organization to its company's Microsoft sign-in, and new members to addresses on its domains.

- Roles in the organization (owner, administrator, member, read only); the Customer can reserve a campaign's sensitive documents to its requester and its administrators; downloads and previews of sensitive documents, recorded in each campaign's log, can be viewed by its administrators.

Annex 2: sub-processors and places of processing

- Hostinger International Ltd (Cyprus, server in France): hosting of the service and the database; local copy of recently received files, encrypted, for a few days.

- Brevo (Sendinblue SAS, France): delivery of the emails and text messages sent to contributors. If the Customer chooses to send from its own domain name, that domain is declared at Brevo and authenticated by the DNS records the Customer creates.

- Merci Facteur (a service of Bourdet, France): only if the Client places postal sends (letter, registered letter with acknowledgement of receipt, postcard) in the sequence of a campaign. Printing and handing over to La Poste; receives, at the time of each send, the contributor's name and postal address and the document to print (with, for a postcard, the photo chosen by the Client, who warrants having the right to use it); erasure of this data requested 15 days after printing.

- Scaleway (Scaleway SAS, France, Paris data centre): storage of the files received and of the database backups (a continuous copy and an hourly copy), all encrypted by PAPEL before sending: Scaleway cannot read them. A file deleted from the service is erased there straight away; its former versions and the backups disappear 30 days later at the most.

- Twilio (Twilio Inc., United States): only if the Client places a "Call" step in the sequence of a campaign. Voice calls with a synthetic voice; receives, at the time of each call, the contributor's phone number and the text of the message read out; calls are never recorded. Transfer outside the European Union covered by section 12.

- ElevenLabs (Eleven Labs Inc., United States, and its affiliates), with Google's Gemini language model as a further subprocessor of ElevenLabs: only if the Client places a "Call by an agent" step in the sequence of a campaign. Automated voice agent that talks with the contributor, through the service's Twilio number; receives, at the time of each call, the contributor's phone number, first name and greeting, language and tone, the name of the Client (requester) and of the campaign, the list of expected documents with their format and short instructions, the deadline and the number of messages already sent; returns the call status, its duration, a summary and the written transcript, kept with the campaign and deleted with it. Agent set with no audio recording and the shortest retention offered by ElevenLabs; conversation deleted at ElevenLabs as soon as its result is received. Processing may take place outside the European Union, in particular in the United States, covered by section 12.

- Cloudflare: domain name management (DNS) only; no contributor data goes through it.

- Documenso: electronic signature software installed on PAPEL's servers, at Hostinger; it is not a third party.

- Anthropic (Anthropic PBC, United States): only if the Customer turns on AI document review, which is off by default. Analysis of the reduced image, or the first three pages, of each document received, with the name and instructions of the requested document, never the contributor's name or contact details; no file is stored at Anthropic, and the data is not used to train its models; sensitive documents only if the Customer expressly allows it with a second checkbox. Transfer outside the European Union covered by section 12. The provider in use is shown in "My settings"; any change of provider is announced under the last paragraph of this section.

- Mistral AI (Mistral AI SAS, France): only if the Client uses "Tell me in a voice note" when creating a campaign. Transcription of the recording, sent at the time of transcription and never kept by PAPEL;

the resulting text is sent to Anthropic (United States, transfer covered by section 12) to suggest campaign scenarios and is only kept with the campaign created.

Signatures

For the Client: _____

Name, position, date and signature: _____

For PAPEL SAS

Name, position, date and signature: _____

Reference text: https://pleasesendit.com/dpa, version of 2026-10-04, SHA-256 fingerprint of the page 28dbdb368695308c8ce350bbf24c4b2f611fd8c6a55cc0b8b82110ecef140d61.