LEGAL DOCUMENT

Data Processing Agreement

Version dated 2026-10-25 · ALK Innovations · Trupeo

In short

When your team uses Trupeo, ALK Innovations processes the mail of your connected mailboxes on your behalf. You are the controller of that data and we are your processor. Article 28 of the GDPR requires a contract between the two: this is it.

Nothing to sign. This agreement forms part of our Terms of Service: accepting them accepts it. If your data protection officer wants a copy signed by us, ask for one through our contact form.

The European Commission's clauses, unchanged. The body of this agreement is the standard contractual clauses the European Commission adopted for controllers and processors, word for word. What is specific to Trupeo is in the annexes: what we process, how we protect it, and who helps us do it.

Few service providers touch your mail. Microsoft Azure hosts Trupeo in France and Amazon SES sends the emails Trupeo writes to your team. Google Cloud only passes on Gmail's notice that a mailbox has changed. We tell you 30 days before adding or replacing one, and you can object.

Your mail stays yours. We process it only to provide the service, on your instructions. We do not sell it, we do not use it for advertising, and we do not train artificial intelligence on it.

The detailed version is available below.

Detailed version

Table of contents

1. How this agreement applies
2. Section I: general provisions
3. Section II: obligations of the parties
4. Section III: final provisions
5. Annex I: list of parties
6. Annex II: description of the processing

7. Annex III: technical and organisational measures
8. Annex IV: list of sub-processors

1. How this agreement applies

This Data Processing Agreement (hereinafter "the Agreement") forms part of the Terms of Service between **ALK Innovations** and the Client. It applies to the personal data that ALK Innovations processes on behalf of the Client when it provides the **Trupeo** Service, as described in Annex II. The words Client and Service have the meaning the Terms of Service give them.

The parties

The Client is the controller and ALK Innovations is its processor. In the clauses below, "the controller" is the Client and "the processor" is ALK Innovations.

The standard contractual clauses

Parts 2 to 4 reproduce, without changing them, the standard contractual clauses between controllers and processors adopted by the European Commission in Implementing Decision (EU) 2021/915 of 4 June 2021 (hereinafter "the Clauses"). Parts 5 to 8 are their Annexes I to IV. Where the Clauses leave a choice, the parties have chosen Regulation (EU) 2016/679 (the GDPR) rather than Regulation (EU) 2018/1725, which applies only to the institutions and bodies of the European Union, and, in Clause 7.7, the general written authorisation, with 30 days' notice. The optional Clause 5 is not used.

Acceptance

The Client accepts this Agreement by accepting the Terms of Service, without having to sign it. For a Client who accepted the Terms of Service before 24 October 2026, this Agreement applies from that date. It creates obligations for ALK Innovations only, and therefore takes effect on its publication, without the notice of Article 21 of the Terms of Service. ALK Innovations provides a copy signed on its behalf to any Client who asks for one through the contact form.

The Client's documented instructions

The Client's instructions, within the meaning of Clause 7.1, are this Agreement, the Terms of Service, and what the Client's users do in the Service and in its settings: connecting a mailbox, inviting or removing a member, writing, assigning, filing or trashing a conversation, exporting data, connecting an assistant, and so on.

Connecting an assistant such as Claude or ChatGPT to a Trupeo account is an instruction to make data available to that assistant, within the rights of the user who connected it. The assistant then acts under the responsibility of the company that runs it, under that company's own terms: it is not a sub-processor of ALK Innovations.

What this Agreement does not cover

ALK Innovations is not the Client's processor, but a controller in its own right, for the processing it carries out for its own purposes: managing user accounts, billing, the security of the Service,

handling the requests users send to the Trupeo team, audience and product-use measurement, and customer relationship management. That processing is described in the Privacy Policy, which governs it.

Changes and other provisions

ALK Innovations keeps the Annexes up to date as the Service changes, which Clause 2 allows. A change to the list of sub-processors follows Clause 7.7: the owner of each mailbox is informed of it by email at least 30 days in advance. Any other change follows Article 21 of the Terms of Service. Everything this Agreement does not settle, including the governing law and the competent jurisdiction, is settled by the Terms of Service; in the event of a contradiction, Clause 4 makes the Clauses prevail.

2. Section I: general provisions

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: Docking clause (optional)

This optional clause is not used in this agreement.

3. 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) 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 30 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.

4. 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.

5. Annex I: list of parties

Controller

Name: the Client, that is the organisation that subscribed to the Service, as identified in its Trupeo account and in its billing details.

Address: the address given in the Client's billing details.

Contact person's name, position and contact details: the owner of each mailbox the Client has connected, at the email address of their Trupeo account. A Client that has appointed a data protection officer can give their details through the contact form.

Signature and accession date: the date on which the Client accepted the Terms of Service or, for a Client that had accepted them before, 24 October 2026.

Processor

Name: ALK Innovations, a SASU with a capital of €1,000, registered with the Nantes RCS under number 983 856 642.

Address: 31 avenue des Korrigans, 44300 Nantes, France.

Contact person's name, position and contact details: Quentin Georget, President of ALK Innovations and its point of contact for the protection of personal data, through the contact form (by selecting "GDPR Request") or by post at the address above. ALK Innovations has not appointed a data protection officer.

Signature and accession date: the publication of this Agreement, on 24 October 2026.

6. Annex II: description of the processing

Categories of data subjects whose personal data is processed

- The Client's users: the members of each of its shared mailboxes, and the people invited to join one.
- The Client's correspondents: the senders and recipients of the mail of its connected mailboxes, and anyone that mail or its attachments name.
- The people in the address book of each mailbox, including the contacts kept the same as Google Contacts or Outlook.

Depending on the Client's activity, these people may include minors, notably for an educational institution.

Categories of personal data processed

- **Mail**: the messages of each connected mailbox (subject, body, senders, recipients, dates, attachments, labels and folders), and the mail the Client's users write and send through the Service.
- **The connection to each mailbox**: its address, and what Trupeo connects to it with (the access granted by Google or Microsoft, or the IMAP and SMTP login details).
- **What the team writes and does in Trupeo**: team notes, assignments, statuses, labels, scopes, signatures, and the history of these actions with the member who took each one.
- **The address book**: the addresses read off the mail with the name each message gives, the number and dates of exchanges, what the team adds (name, company, job title, phone numbers, note), contact groups and, where it is turned on, the contacts exchanged with Google Contacts or Outlook.
- **The members as their teammates see them**: name, email address and profile picture.

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

ALK Innovations neither asks for sensitive data nor seeks it out, but mail can contain some, as can anything a correspondent writes. It is protected like all mail, with these restrictions:

- strict purpose limitation: mail is processed only to provide the Service, never for advertising, and never to train artificial intelligence models;
- the text of messages and the attachments are encrypted with a key specific to each mailbox (Annex III);
- only the members the Client gives access to a mailbox see it, within the scopes the Client sets;
- nobody at ALK Innovations reads mail, except at the Client's explicit request to handle a support request, where necessary for security purposes such as investigating abuse, or to comply with a legal obligation, and every time the Trupeo team opens an account, it is recorded (Annex III).

Nature of the processing

Collecting the mail from the Client's email provider (through the Gmail API, Microsoft Graph, or IMAP and SMTP), storing, organising and displaying it to the members, searching it, sending mail on the Client's behalf, applying at the provider the actions the members take in Trupeo (read, archive, trash, spam), keeping the address book the same as Google Contacts or Outlook where that is turned on, notifying the members (in the app, by email and on their devices), exporting data at the Client's request, and erasing it.

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

Providing the Client with the Service described in the Terms of Service: a shared mailbox in which the Client's team reads, distributes, follows and answers the mail of its connected mailboxes. And, for that Service only: looking into the Client's mailboxes when the Client asks for it to answer one of its support requests, and keeping the Service secure.

Duration of the processing

For the duration of the contract. When a subscription ends, the mailbox concerned and its data are deleted at the end of the paid period, or 14 days after termination if that is later, unless the Client reactivates the subscription before then (Article 6 of the Terms of Service). Disconnecting a mailbox deletes the messages and attachments stored for it. Once deleted, the data leaves the database backups within 35 days at most, and the previous copies kept in object storage within 60 days of being written. Nothing is deleted at the Client's email provider when the contract ends: the mail and the contacts stay there.

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

See Annex IV. Each sub-processor processes the data for as long as the processor engages it for that processing, except what Annex IV says one keeps longer.

7. Annex III: technical and organisational measures

These are the measures in place on 24 October 2026. The security page sets them out with their limits and their dates.

Encryption of personal data

- Microsoft Azure encrypts the database and the file storage.
- Trupeo also encrypts some data itself (AES-256-GCM): since 10 July 2026, the text of messages and the attachments, with a key for each mailbox, and the mailbox login details, with a key of the service. The secrets these keys come from are kept in Azure Key Vault, apart from the storage: copying a file out of storage is not enough to read it.
- A message's subject, its addresses, its preview and what the team writes in Trupeo are encrypted by Azure only.

Protection of data during transmission

- The site and the app are served over HTTPS only. Trupeo's connections to Google and Microsoft are encrypted.
- Its connections to an IMAP or SMTP server are encrypted when that server offers it. Trupeo does not refuse a server that does not: the Client chooses its server.

User identification and authorisation

- Each member signs in with their own account, with a password or with their Google or Microsoft account. An account with a password can turn on two-step verification: a code from an authenticator app, with ten backup codes.
- A mailbox is shared only with the people its owner invites. The owner can limit a member to the conversations filed in some scopes. A member removed from a mailbox loses access to it at once.
- Each account lists its signed-in sessions, so that its user can recognise their devices.

Access by ALK Innovations' personnel

- Nobody at ALK Innovations reads mail, except in the cases set out in Annex II.
- Every time a member of the Trupeo team opens an account, it is recorded, with the date, and shown to that account's user in their settings. Should that record fail to be written, the opening is still entered in the service's logs.
- For Gmail, Trupeo was never granted the permission to delete an email permanently.

Physical security of the locations where data is processed

- Trupeo runs on Microsoft Azure: the database, the application servers, and the stored message bodies and attachments are in France (Azure France Central region). The physical security of the data centres is Microsoft's.

Availability and restoration

- The database is backed up every day, and the backups are kept for up to 35 days.
- Restoring has been rehearsed: on 3 September 2026, a restored database was read back and decrypted with the real key.

Regular testing and evaluation

- An independent lab, TAC Security, authorised by the App Defense Alliance, assessed Trupeo under Google's CASA programme: compliant at level AL1 since 11 September 2026, across 20 control groups. The assessment is renewed every year.
- Anyone can report a security flaw through the reporting page, under a published policy.

Events logging

- Each conversation keeps the history of what was done in it, by whom and when.

- Each opening of an account by the Trupeo team, and each data export request with its date and the IP address it came from, is recorded.
- Technical logs are kept for security and to detect incidents.

Data minimisation and limited retention

- Trupeo stores the content of a message it receives only from the moment someone opens it; the email provider keeps the original. What the team writes in Trupeo, drafts and sent mail included, is stored as it is written.
- The retention periods are those of Annex II. Deleting a mailbox also purges the files stored for it, and an export file is deleted seven days after it is ready.

Data portability and erasure

- The owner of a mailbox can export its data from its settings, as structured, machine-readable data: the mailbox and its settings, its members, every conversation and message with senders, recipients, subject and dates, the team notes, the address book, the activity history and the list of attachments. Ticking "Include the content of the emails and the attachments Trupeo stores" adds the message bodies Trupeo holds, decrypted, the drafts and the stored attachment files; the body of a message nobody opened in Trupeo is not in it, and the email provider keeps the original.
- The owner of a mailbox can delete it from its settings, which erases everything stored for it, and every user can delete their own account from theirs.
- Once a deleted mailbox's stored files are purged, each of its owners receives an email certifying the deletion, with its date and the date by which the database backups and the file storage's previous versions that still hold some of it are gone. The address and language it is sent to are kept only until it is sent.

Assistance to the controller (Clauses 8 and 9)

- Requests from data subjects: the Client can answer most of them itself with the export and erasure tools above. For anything they do not cover, the Client can ask ALK Innovations for assistance through the contact form (by selecting "GDPR Request"), and ALK Innovations answers within 30 days at most.
- Personal data breach: ALK Innovations notifies the owner of each mailbox concerned by email, with the elements of Clause 9.2. The contact point for more information is the one in Annex I.
- Impact assessments and prior consultations: on request, ALK Innovations provides the information it holds about the processing, including this Agreement, the security page and the result of its CASA assessment.

8. Annex IV: list of sub-processors

The Client authorises the sub-processors below, which form the agreed list of Clause 7.7(a). ALK Innovations informs the owner of each mailbox by email at least 30 days before adding one to the list or replacing one.

Sub-processor	Processing on behalf of the Client	Country
Microsoft Azure (Microsoft France SAS)	Hosting the Service: application servers, database, storage of message bodies and attachments, backups and key storage	France
Amazon Web Services EMEA SARL (Amazon SES)	Sending the emails Trupeo writes to the Client's users: invitations and notifications. A notification email may carry a conversation's subject and the sender's name, never the message body	Ireland
Google LLC (Google Cloud Pub/Sub)	For a Gmail mailbox only, carrying to Trupeo Gmail's notice that the mailbox has changed: its address and a change number, never its mail	USA

Microsoft France SAS and Amazon Web Services EMEA SARL process the data in the European Union. Amazon SES keeps on a suppression list the addresses whose mail bounced for good or that reported a mail as spam, so as not to write to them again, and that list outlasts the contract. The transfer to Google LLC relies on the safeguards described in the Privacy Policy, as Clause 7.8 provides.

Who is not a sub-processor

- Google, Microsoft and the Client's other email providers already hold the Client's mailbox, under the Client's own contract with them: Trupeo connects to them on the Client's instructions.
- The services that deliver notifications to a member's device are those of the browser the member uses (Google, Mozilla, Apple or Microsoft): the browser chooses them, not ALK Innovations. They receive the address of that device's subscription and content encrypted end to end, which they cannot read.
- An assistant a user connects to their account acts under the responsibility of the company that runs it, as part 1 sets out.

This English version is provided for convenience. In case of any inconsistency, the French version prevails.