AVIOVERSE

DOCUMENT
Trust pack

EDITION
2026-11-13

Avioverse trust pack

Company details, how we protect data, our sub-processors and the data processing agreement

1. Company

Legal name: AVIOVERSE LTD
Registration number: HE 499684
Registered with: Department of Registrar of Companies and Intellectual Property, Cyprus
Registered office: Agiou Efraim, 1A, Pera Chorio, 2572, Nicosia, Cyprus
Privacy contact: privacy@avioverse.aero
Security contact: security@avioverse.aero

2. How we protect data

Each statement below can be checked. The same list is Annex III of the data processing agreement and is published at https://avioverse.aero/security.

Where data is kept

- The application and the database run on two servers in a Hetzner data centre in Falkenstein, Germany.
- Uploaded files are stored in Cloudflare R2 object storage in the European Union.
- Backups are stored in Hetzner Object Storage in Nuremberg, Germany.
- Avioverse runs no data centre of its own. Hetzner and Cloudflare provide the physical security of these locations.

Encryption

- All traffic to and from Avioverse uses HTTPS.
- Traffic between the application server and the database server travels over an encrypted private link.
- Backups are encrypted before they are stored. The keys to restore them are held away from the application servers.

Network and servers

- The servers open no port to the internet for the application. Requests arrive through an outbound-only Cloudflare tunnel.
- The database and the search index accept connections only over the private link between the two servers.
- Server administration is limited to the operator, by a firewall rule and Cloudflare Access.
- Requests to the service are rate-limited.
- An outside monitor checks the website, the application and the API, and each server reports its own health every five minutes.

Sign-in and access

- People sign in with a one-time code sent to their email address, or with Google. Avioverse stores no passwords.

- Every request to a workspace is checked on the server against the person's membership and role. Team owners and admins manage members and roles.
- Each account's files are kept under its own storage prefix and are read through signed addresses.
- The administration console is a separate application behind Cloudflare Access, open to named operators only.

Backups and recovery

- Every change to the database is archived continuously, with a daily differential copy and a full copy at least every fourteen days.
- Files and server settings are copied every hour.
- Backups are kept apart from the working servers, which cannot delete or overwrite them.
- A separate monitor alerts the operator when a backup fails or stops reporting.
- After a recovery, records, files and settings are restored together and checked before the service reopens.

Testing

- A complete restore onto a separate clean server was carried out on 2026-10-10 and twice on 2026-10-23. The policy is to repeat it every month and after a change to keys, backup tools, database images or storage.
- Every release is built from a version that has passed automated tests and a scan of its dependencies, secrets, code and container files. No image is built unless the scan passes, and each image is scanned again before it is published.
- The public addresses are scanned every week with a baseline web scan.

Updates

- The servers install operating-system security updates automatically every day.
- The third-party software the application uses is checked for known vulnerabilities at every release and every week.

Record history and error reports

- Audits and forms keep a history of review decisions and changes, and forms and procedures record every change of who has access. Every AI generation is logged.
- Error reports go to Sentry in the European Union with passwords and keys removed, and without request contents, account profiles or screen recordings.

Responsibility

- A named operator is responsible for the service: investigates alerts, records recovery tests and authorises reopening after a recovery.
- Security problems are reported to security@avioverse.aero.
- Avioverse notifies affected customers of a personal data breach as the GDPR requires.

AI providers

- AI providers receive only the prompts, documents and context needed for the request a person makes.
- Avioverse does not use customer content to train AI models, and requires its providers to process it only to provide the service.
- Sharing data with Voyage AI for model improvement is switched off in the Avioverse account.

Deletion and retention

- A deleted account is erased after a 30-day window in which it can be restored.
- Erased data can remain in encrypted backups for about 35 days, plus the storage provider's processing time.
- After a recovery from backup, erasures made after the recovery point are applied again before the service reopens.

Export

- "Download my data" gives a machine-readable copy of an account at any time.
- Account deletion is self-serve.

3. Data processing agreement

The agreement is concluded online inside Avioverse, under Agreements: in Team settings by the Team's owner or an admin, or in account settings for a personal workspace. This is its standard text, version of 2026-11-13; Annex IV is the list of sub-processors of 2026-11-13.

This agreement consists of the standard contractual clauses between controllers and processors adopted by the European Commission in Commission Implementing Decision (EU) 2021/915 of 4 June 2021 (OJ L 199, 7.6.2021, p. 18), with their wording unchanged, the choices below and Annexes I to IV.

Choices made where the clauses offer options

Clauses 1(a), 8(c)(4), 9.1(b), 9.1(c) and 9.2: Option 1: Regulation (EU) 2016/679 (the General Data Protection Regulation) applies.

Clause 5 (docking clause, optional): Included.

Clause 7.7(a): Option 2: general written authorisation. The processor announces a new or replaced sub-processor at least 30 days in advance.

STANDARD CONTRACTUAL CLAUSES

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 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.

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):

The customer’s details, entered when the agreement is concluded: a person’s name and address, or a company’s legal name, registered address, registration number, and the name and position of the person who concludes it. The date and time are recorded with them.

Processor(s):

Name: AVIOVERSE LTD, registration number HE 499684

Address: Agiou Efraim, 1A, Pera Chorio, 2572, Nicosia, Cyprus

Contact person’s name, position and contact details: Privacy contact, privacy@avioverse.aero

Signature and accession date: AVIOVERSE LTD offers these Clauses as its standard agreement and is bound by them from the date and time the controller concludes them.

ANNEX II

Description of the processing

Categories of data subjects whose personal data is processed

- People who use the controller's workspace: the account holder and, in a Team, its members and invited guests.
- People named in the records and files the controller keeps in the workspace, for example employees, contractors, trainees, licence holders, auditors and auditees, contact persons at suppliers and customers, and people named in reports.

Categories of personal data processed

- Identification and contact details: name, email address, organisation, role or position.
- Professional records: licences, authorisations, certificates, training and qualification records, and who created, changed, reviewed or approved a record, and when.
- The content the controller creates, uploads or shares: tasks, procedures, forms and responses, audits and findings, risk records, registers, safety and occurrence reports, files, comments, and conversations with the assistant.

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- The service is not designed for special categories of personal data and does not ask for them. The controller decides what its records contain; a safety or occurrence report may, for example, mention a person's health.
- Such data is processed only to provide the feature a user asks for, under the same measures as all other content (Annex III): access is limited to the members of the workspace, it is not used to profile anyone, and it is not used to train AI models.

Nature of the processing

- Storing, organising, displaying, searching, transmitting and deleting the content; reading uploaded documents, including scanned pages; producing answers, drafts and extractions with AI models when a user asks; sending service emails and notifications; and making encrypted backups.

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

- To provide the Avioverse workspace and its assistant to the controller under the Avioverse Terms of Service, on the instructions the controller gives by using the service.

Duration of the processing

- For as long as the controller keeps the workspace. When the controller deletes a record, a Team or the account, the data is erased as the Avioverse privacy notice describes; encrypted backup copies then expire within about 35 days, plus the storage provider's processing time.

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

- Each sub-processor in Annex IV processes the data named beside it, for the purpose named beside it, for as long as the processor uses it to provide the service.

ANNEX III

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

Measures for ensuring physical security of locations at which personal data are processed

- The application and the database run on two servers in a Hetzner data centre in Falkenstein, Germany.
- Uploaded files are stored in Cloudflare R2 object storage in the European Union.
- Backups are stored in Hetzner Object Storage in Nuremberg, Germany.
- Avioverse runs no data centre of its own. Hetzner and Cloudflare provide the physical security of these locations.

Measures of pseudonymisation and encryption of personal data

- All traffic to and from Avioverse uses HTTPS.
- Traffic between the application server and the database server travels over an encrypted private link.
- Backups are encrypted before they are stored. The keys to restore them are held away from the application servers.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

- The servers open no port to the internet for the application. Requests arrive through an outbound-only Cloudflare tunnel.
- The database and the search index accept connections only over the private link between the two servers.
- Server administration is limited to the operator, by a firewall rule and Cloudflare Access.
- Requests to the service are rate-limited.
- An outside monitor checks the website, the application and the API, and each server reports its own health every five minutes.

Measures for user identification and authorisation

- People sign in with a one-time code sent to their email address, or with Google. Avioverse stores no passwords.
- Every request to a workspace is checked on the server against the person’s membership and role. Team owners and admins manage members and roles.
- Each account’s files are kept under its own storage prefix and are read through signed addresses.
- The administration console is a separate application behind Cloudflare Access, open to named operators only.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

- Every change to the database is archived continuously, with a daily differential copy and a full copy at least every fourteen days.
- Files and server settings are copied every hour.
- Backups are kept apart from the working servers, which cannot delete or overwrite them.
- A separate monitor alerts the operator when a backup fails or stops reporting.
- After a recovery, records, files and settings are restored together and checked before the service reopens.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

- A complete restore onto a separate clean server was carried out on 2026-10-10 and twice on 2026-10-23. The policy is to repeat it every month and after a change to keys, backup tools, database images or storage.
- Every release is built from a version that has passed automated tests and a scan of its dependencies, secrets, code and container files. No image is built unless the scan passes, and each image is scanned again before it is published.
- The public addresses are scanned every week with a baseline web scan.

Measures for ensuring system configuration, including default configuration

- The servers install operating-system security updates automatically every day.
- The third-party software the application uses is checked for known vulnerabilities at every release and every week.

Measures for ensuring events logging

- Audits and forms keep a history of review decisions and changes, and forms and procedures record every change of who has access. Every AI generation is logged.
- Error reports go to Sentry in the European Union with passwords and keys removed, and without request contents, account profiles or screen recordings.

Measures for internal IT and IT security governance and management

- A named operator is responsible for the service: investigates alerts, records recovery tests and authorises reopening after a recovery.
- Security problems are reported to security@avioverse.aero.
- Avioverse notifies affected customers of a personal data breach as the GDPR requires.

Measures for ensuring data minimisation

- AI providers receive only the prompts, documents and context needed for the request a person makes.
- Avioverse does not use customer content to train AI models, and requires its providers to process it only to provide the service.
- Sharing data with Voyage AI for model improvement is switched off in the Avioverse account.

Measures for ensuring limited data retention

- A deleted account is erased after a 30-day window in which it can be restored.
- Erased data can remain in encrypted backups for about 35 days, plus the storage provider’s processing time.
- After a recovery from backup, erasures made after the recovery point are applied again before the service reopens.

Measures for allowing data portability and ensuring erasure

- “Download my data” gives a machine-readable copy of an account at any time.
- Account deletion is self-serve.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller

The processor engages each sub-processor in Annex IV under that provider’s data processing terms, which bind it to protect the data and to assist as these Clauses require.

Description of the specific technical and organisational measures to be taken by the processor to be able to provide assistance to the controller.

- The controller can read, correct, export and delete the personal data in its workspace itself, at any time.
- When a data subject writes to the processor about data the controller keeps in its workspace, the processor passes the request to the controller’s contact in Annex I and does not answer it itself.
- The processor answers the controller’s requests for help with data subject requests, impact assessments and consultations with a supervisory authority at privacy@avioverse.aero.
- The processor reports a personal data breach to the controller’s contact in Annex I by email without undue delay, with the information listed in Clause 9.2.

ANNEX IV

List of sub-processors

The controller has authorised the use of the following sub-processors:

Sub-processor	Processing	Data	Location and transfer basis
Hetzner Online Hetzner Online GmbH, Germany	Servers, database, file storage and backups	All account, workspace and file data	European Union (Germany or Finland); backups in Nuremberg, Germany
Cloudflare Cloudflare, Inc., United States	Domain name service, secure network entry, primary file storage, reading uploaded documents (extracting text and preparing scanned pages), PDF rendering, independent backup monitoring and the early-access list	Service traffic, uploaded and shared files, exported documents, aggregate backup health and early-access email addresses	Global network; primary files and early-access list stored in the EU; United States company Transfer basis: EU-U.S. Data Privacy Framework; otherwise standard contractual clauses (Decision (EU) 2021/914)
Stripe Stripe Payments Europe, Limited, Ireland	Payments, subscriptions, invoices and tax calculation	Name, email, billing address, payment details and transaction history	Ireland and the United States Transfer basis: To Stripe, LLC in the United States: Data Privacy Framework; otherwise standard contractual clauses (Decision (EU) 2021/914)
Resend Plus Five Five, Inc., United States	Service email: sign-in codes, invitations, notifications and account notices	Email address, name and the content of the message	Ireland, European Union (sending region) Transfer basis: Standard contractual clauses (Decision (EU) 2021/914) and the EU-U.S. Data Privacy Framework
OpenAI OpenAI Ireland Ltd., Ireland	AI answers, document extraction and drafting, answer checking, and transcribing Telegram voice notes	Prompts, documents, audio and context sent with the request	United States Transfer basis: Onward transfers outside the European Economic Area: standard contractual clauses or an adequacy decision
Anthropic Anthropic Ireland, Limited, Ireland	AI answers, including when another model is unavailable, and checking answers against their sources	Prompts, documents and context sent with the request	United States Transfer basis: Standard contractual clauses (Decision (EU) 2021/914)
Google (Gemini API) Google Cloud EMEA Limited, Ireland	Reading scanned documents (OCR)	Documents and prompts sent with the request	United States Transfer basis: To the United States: EU-U.S. Data Privacy Framework; otherwise standard contractual clauses
Voyage AI Voyage AI Innovations, Inc.	Search indexing and ranking of your saved content and your questions	Text of your content and queries	United States Transfer basis: Standard contractual clauses (Decision (EU) 2021/914)
Tavily AlphaAI Technologies Inc., United States	Live web search when the assistant searches the web for you	Search queries written from your request	United States Transfer basis: Standard contractual clauses
Daytona Daytona Platforms Inc., United States	Isolated sandboxes that run code the assistant writes to analyse your data	The files and data you ask it to analyse	United States Transfer basis: Standard contractual clauses (Decision (EU) 2021/914)

Sub-processor	Processing	Data	Location and transfer basis
Sentry Functional Software, Inc., United States	Reports of errors in our servers and in the web app in your browser, so we can find and fix them	Error type, a shortened error message with passwords and keys removed, where in our code it happened and, for the web app, the page it was on with record numbers and search terms removed; reports from your browser pass through our servers, so Sentry does not receive your IP address or browser details; never request contents, account profiles or screen recordings	European Union (Frankfurt, Germany); account and project settings in the United States; United States company Transfer basis: EU-U.S. Data Privacy Framework; otherwise standard contractual clauses (Decision (EU) 2021/914)

List of 2026-11-13. A new or replaced sub-processor is announced at least 30 days in advance.