ATELYR

Data Processing Agreement

Version 1 - Effective date 1st of May 2026

1. Parties

This Data Processing Agreement (hereinafter: "DPA") is entered into between:

1.1 Controller

The Partner or End Customer that has entered into the Main Agreement with Atelyr and has accepted the applicable terms, and that has personal data processed by Atelyr (hereinafter: "Controller"). The identity of the Controller follows from the account registration with Atelyr.

1.2 Processor

Atelyr B.V.
Dorpsstraat 324A, 1531 HW Wormer, Netherlands
Chamber of Commerce number: 99674327
Email: privacy@atelyr.ai
Website: www.atelyr.ai

(hereinafter: "Atelyr" or "Processor")

For privacy-related questions in the context of this DPA, the Controller may also contact Atelyr's Data Protection Officer:

Data Protection Officer
Email: dpo@atelyr.ai
Post: Atelyr B.V., Attn. Data Protection Officer, Dorpsstraat 324A, 1531 HW Wormer, Netherlands

The Controller and the Processor are together referred to as "the parties".

1.3 Controller's point of contact

The Controller designates a contact person for privacy-related communications in the context of this DPA and communicates their contact details to Atelyr via privacy@atelyr.ai.

The Controller is responsible for keeping these details up to date. In the absence of a designated contact person, all Users with the role of "admin" or "owner" within the Software shall serve as the point of contact, each individually and jointly, such that contact with any one of them is sufficient.

ATELYR

2. Whereas

2.1 The parties have entered into an Agreement under which Atelyr makes the Software available to the Controller (the "Main Agreement").

2.2 In the performance of the Main Agreement, Atelyr processes personal data on behalf of and for the benefit of the Controller, within the meaning of Article 28 of the General Data Protection Regulation (GDPR).

2.3 In this DPA, the parties set out the terms under which Atelyr processes personal data on behalf of the Controller.

2.4 This DPA forms part of and supplements the Main Agreement. In the event of conflict, this DPA prevails to the extent it concerns the processing of personal data.

3. Definitions

In this DPA, the following terms have the following meanings:

- **AI Provider:** a third-party provider of generative AI services used within the Software, either selected and configured by Atelyr, or independently chosen by the Controller.
- **Data Breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data, as referred to in Article 4(12) GDPR.
- **Data Subject:** the natural person to whom the personal data relates.
- **End User:** the natural person who, through the Software, interacts with an AI agent deployed by the Controller, including but not limited to a voice agent, chatbot, or other automated conversational application, and whose personal data (including voice, conversation content, and metadata) is processed in that context. The End User is not a contracting party of Atelyr.
- **GDPR:** Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).
- **Personal Data:** any information relating to an identified or identifiable natural person, as referred to in Article 4(1) GDPR.
- **Processing:** any operation or set of operations performed on personal data, as referred to in Article 4(2) GDPR.
- **Software:** the platform and applications of Atelyr that the Controller uses under the Main Agreement.
- **Sub-processor:** a third party engaged by Atelyr to process personal data on behalf of the Controller.
- **User:** the natural person who, on behalf of the Controller, has access to the Software or the Partner Portal, such as an employee or freelancer.

4. Scope and Duration

4.1 Atelyr processes personal data solely for the purpose of performing the Main Agreement and in accordance with the documented instructions of the Controller, unless a legal obligation requires otherwise.

4.2 The nature and purpose of the processing activities, the categories of data subjects, and the categories of personal data are set out in Annex A to this DPA.

4.3 This DPA enters into force at the moment the Controller accepts the applicable terms upon entering into the Main Agreement, and remains in effect for as long as Atelyr processes personal data on behalf of the Controller, but no longer than until termination of the Main Agreement.

4.4 If a legal obligation requires Atelyr to process personal data outside the Controller's instructions, Atelyr will notify the Controller in advance, unless the law prohibits such notification.

5. Obligations of Atelyr

5.1 Atelyr processes personal data solely on the basis of documented instructions from the Controller, unless a provision of Union or Member State law applicable to Atelyr requires otherwise. For the purposes of this DPA, the configuration and use of the Software by the Controller constitute the Controller's documented instructions. The Controller may only provide instructions through the functionalities available within the Software.

5.2 Atelyr ensures that persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory obligation of confidentiality. This confidentiality obligation remains in force after termination of the employment or engagement of the relevant person.

5.3 Atelyr applies measures tailored to the nature and risk of the relevant processing. These measures may include, among others:

- encryption of personal data;
- access control and authentication;
- monitoring and logging;
- backup and recovery;
- periodic security audits;
- incident management; and
- awareness and training of employees.

When determining and assessing these measures, Atelyr takes into account the state of the art, the nature and scope of the processing, and the likelihood and severity of the risks to data subjects. Atelyr adjusts the measures as necessary in light of technological developments and changing risks.

5.4 Atelyr provides the Controller with reasonable assistance in fulfilling its obligations under Articles 32 to 36 GDPR, taking into account the nature of the processing and the information available to Atelyr.

5.5 Atelyr makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR, and contributes to audits as referred to in Article 10 of this DPA.

ATELYR

5.6 Atelyr does not use conversation content, audio recordings, or directly identifiable End User data for commercial purposes, profiling, or any purpose other than the performance of the Main Agreement. Atelyr does not use voice recordings to identify individuals based on the unique characteristics of their voice.

6. Automated Decision-Making

6.1 Atelyr does not apply fully automated decision-making, including profiling, that produces legal effects concerning data subjects or similarly significantly affects them within the meaning of Article 22 GDPR.

6.2 The Software uses artificial intelligence for the processing of conversation content and the generation of outputs. This technology is used solely as a supporting tool for the provision of services. Outputs generated by AI do not form the basis for automated decisions with legal effects and are not used for profiling of data subjects.

6.3 If the way in which the Controller uses the Software leads to decisions that significantly affect data subjects, the Controller is itself responsible for compliance with Article 22 GDPR and the obligations arising from it, including providing meaningful information about how the decision is made, enabling human review on request, and giving the data subject the right to challenge the decision.

7. Obligations of the Controller

7.1 The Controller warrants to Atelyr that the processing of personal data it instructs is lawful and does not infringe the rights of data subjects.

7.2 The Controller ensures that there is a valid legal basis for the processing of personal data provided to Atelyr or processed by Atelyr on the Controller's instructions. This includes informing End Users about the processing of their personal data through the Software.

7.3 If the Controller deploys the Software in a context where sensitive personal data may regularly arise in conversations, including data concerning health, religion, political beliefs, or trade union membership, the Controller is responsible for having a valid legal basis for the processing of such data and for informing End Users accordingly.

7.4 If the Controller deploys the Software in a context where minors (persons under the age of 16) may be involved, the Controller is itself responsible for obtaining the required consent from the parent or legal representative and for compliance with the applicable laws and regulations for the protection of minors.

7.5 The Controller indemnifies Atelyr against claims from data subjects or third parties arising from a failure by the Controller to comply with this DPA or the GDPR.

ATELYR

8. Sub-processors

8.1 The Controller hereby grants Atelyr general written authorisation to engage sub-processors. Atelyr will inform the Controller of any intended changes regarding the addition or replacement of sub-processors, giving the Controller the opportunity to object.

8.2 Atelyr imposes on sub-processors the same data protection obligations as those set out in this DPA, in particular by means of a written agreement. If a sub-processor fails to fulfil its obligations, Atelyr remains fully liable to the Controller.

8.3 An up-to-date list of sub-processors engaged by Atelyr is available at docs.atelyr.ai. This list is updated regularly.

8.4 For AI Providers that the Controller independently selects and configures within the Software, Atelyr acts as the contracting party and concludes a data processing agreement with the chosen AI Provider on behalf of the Controller. The selection and configuration of an AI Provider through the Software constitutes a documented instruction from the Controller within the meaning of Article 5.1. By making this explicit choice, the Controller assumes all responsibilities arising from the processing by that provider. Atelyr only facilitates the technical connection and has no control over, or insight into, the processing activities carried out by the relevant AI Provider.

8.5 Atelyr makes available for each available AI Provider the security and compliance information publicly disclosed by that provider, including certifications, data residency, and GDPR status. This information is provided for informational purposes and is supplied by Atelyr as provided by the relevant provider. Atelyr does not warrant the completeness or accuracy of this information. The Controller is itself responsible for assessing that information and for selecting a provider that meets its own security and compliance needs.

9. Transfers Outside the EEA

9.1 Atelyr transfers personal data to a country outside the European Economic Area (EEA) only where necessary for the performance of the Main Agreement and where one of the following appropriate safeguards is in place:

- an adequacy decision by the European Commission for the country concerned, including the EU-US Data Privacy Framework where the recipient is certified under it;
- Standard Contractual Clauses (SCCs) as adopted by the European Commission, together with an assessment of the transfer and any additional measures needed to protect the data; or
- another transfer mechanism recognised by the GDPR, including the derogations for occasional transfers.

9.2 To the extent that End User data is processed via sub-processors selected and configured by Atelyr, Atelyr ensures that such processing takes place exclusively within the EEA.

9.3 If the Controller selects an AI Provider that is established outside the EEA or processes outside the EEA, Atelyr concludes a data processing agreement with that provider on behalf of the Controller, including the applicable transfer safeguards as referred to in Article 9.1. The Controller determines how that provider processes the data and acts as controller with respect to that processing.

9.4 Upon request, Atelyr will provide information about the specific transfer safeguards that apply. Requests may be sent to privacy@atelyr.ai.

9.5 If the Controller is itself established outside the EEA, or accesses the personal data processed through the Software from a location outside the EEA, the Controller is itself responsible for ensuring that a valid transfer basis as referred to in Article 9.1 is in place. Atelyr will, upon request, assist in establishing the necessary safeguards, but bears no responsibility for compliance with transfer rules on the Controller's side.

10. Audits and Inspections

10.1 The Controller has the right to verify, or to have verified by an independent auditor bound by confidentiality, Atelyr's compliance with this DPA.

10.2 The Controller announces an audit at least 30 days in advance in writing. Audits are conducted on business days during office hours and must not disproportionately disrupt Atelyr's normal business operations.

10.3 The costs of an audit are borne by the Controller. Atelyr is entitled to charge a reasonable fee for the time and resources spent on the audit. The applicable rate will be communicated to the Controller in writing prior to the audit. If the audit reveals a material shortcoming on Atelyr's part, the costs charged by Atelyr will be credited.

10.4 Atelyr may fulfil its audit obligation by providing a current certificate from a recognised independent auditor (e.g. ISO 27001 or SOC 2), unless the Controller demonstrates that an additional audit is necessary.

11. Rights of Data Subjects

11.1 Atelyr assists the Controller in handling requests from data subjects to exercise their rights under the GDPR, to the extent that this can reasonably be required of Atelyr.

11.2 Requests from data subjects submitted directly to Atelyr will be forwarded by Atelyr to the Controller as soon as possible, and in any event within five business days, unless the Controller has authorised Atelyr in writing to handle such requests independently.

ATELYR

12. Data Breaches

12.1 Atelyr will notify the Controller without undue delay and in any event within 48 hours of discovery of a Data Breach affecting the personal data processed by Atelyr on the Controller's behalf.

12.2 The notification will include at least: the nature of the Data Breach, the categories and estimated number of data subjects and personal data records concerned, the likely consequences, and the measures Atelyr has taken or proposes to take.

12.3 The Controller is responsible for assessing whether notification to the supervisory authority and/or data subjects is required under Articles 33 and 34 GDPR. Atelyr will provide the necessary assistance for this purpose.

12.4 Atelyr records all Data Breaches internally, regardless of whether notification is required.

13. Confidentiality

13.1 Atelyr treats all personal data processed under this DPA as confidential and does not disclose it to third parties, unless this is necessary for the performance of the Main Agreement, required by law, or the Controller has given prior written consent.

13.2 The confidentiality obligation applies during the term of this DPA and remains in force after its termination.

14. Termination and Return or Deletion of Data

14.1 Upon termination of the Main Agreement, Atelyr deletes all personal data it processes on behalf of the Controller, unless a legal obligation requires retention.

14.2 If the Controller wishes to have personal data returned, it must notify Atelyr of this expressly and in writing no later than 30 days after termination of the Main Agreement. Return takes place to the extent technically feasible within the capabilities of the Software. To the extent that return is not or not fully possible, Atelyr will proceed with deletion.

14.3 In the absence of a timely request for return as referred to in Article 14.2, Atelyr will proceed with deletion.

14.4 If deletion is not technically immediately possible, for example in backups, Atelyr ensures that the relevant data is no longer processed and will be deleted as soon as technically possible. Upon request from the Controller, Atelyr will confirm the deletion in writing, unless the law requires archiving.

ATELYR

15. Liability

15.1 The liability regime set out in the Main Agreement applies to this DPA, it being understood that both parties may be liable to data subjects under Article 82 GDPR.

15.2 Atelyr is not liable for damage arising from processing carried out by Atelyr in accordance with the Controller's instructions.

15.3 Atelyr is not liable for damage arising from processing by an AI Provider that the Controller has independently selected and configured within the Software. The Controller bears all responsibility and liability arising from the processing by that provider, including towards data subjects under Article 82 GDPR.

16. Amendments

16.1 Atelyr reserves the right to amend this DPA. Amendments will be announced to the Controller at least 30 days before the intended effective date, in writing, by email, or via a notice or notification within the Software. The announcement will state the nature of the amendment and whether it constitutes a material change as referred to in Article 16.2.

16.2 An amendment is material if it materially restricts the rights of data subjects, increases the Controller's obligations under this DPA, or significantly changes the purposes or categories of processing set out in Annex A. In the event of a material amendment, the Controller has the right to terminate the Main Agreement in writing with effect from the date on which the amendment takes effect. Continued use of the Software after that date constitutes acceptance of the amended DPA.

16.3 Non-material amendments, including editorial adjustments, clarifications, and administrative updates, take effect on the date stated in the announcement. Continued use of the Software after that date constitutes acceptance.

16.4 Amendments that result solely from changes in applicable laws or regulations or a binding decision by a supervisory authority will be implemented as soon as possible and take effect on the date determined by the relevant law or regulation, even if the 30-day notice period cannot be observed. Such amendments do not give rise to a right of early termination of the Main Agreement.

17. General Provisions

17.1 This DPA is governed by Dutch law. Disputes will be submitted to the competent court in the district of Noord-Holland.

17.2 If any provision of this DPA is void or voidable, this does not affect the validity of the remaining provisions. The parties will consult to replace the void or voidable provision with a valid provision that as closely as possible reflects the same intent.

ATELYR

17.3 For questions about this DPA, please contact privacy@atelyr.ai.

Annex A - Processing Activities

The table below describes the processing activities carried out by Atelyr on behalf of the Controller in the context of the Main Agreement.

Categories of data subjects	**Categories of personal data**	**Purposes**	**Retention period**
Users (employees/freelancers of the Controller)	Name, email address, telephone number, job title, company name, username, encrypted password	Access to and use of the Software and the Partner Portal; customer service; onboarding and training	Duration of the Agreement + 1 year; for contracts and acceptance records: 5 years after termination
Users	IP address, device data, browser and operating system information, usage statistics, session data, log files, error messages	Technical management, security, fraud prevention, product development (anonymised)	Log files: maximum 12 months; usage statistics: maximum 3 years
End Users (callers/chat users of the Controller's AI agent)	Audio recordings of conversations; AI-generated transcripts and summaries; interaction metadata (date, duration, participants, channel-specific identifiers such as phone number or session ID); personal data spoken or written during interactions	Service delivery through the Software on behalf of the Controller	Maximum 90 days after the conversation, unless: (i) longer retention is necessary for an ongoing dispute, complaint, or support request (for the duration of handling), or (ii) the Controller has expressly consented to longer retention (consent may be withdrawn, after which deletion takes place within 30 days)
Controller (billing)	Billing address, payment history, invoice data	Invoicing and payment processing	7 years (statutory tax retention obligation)

This overview is indicative. The actual processing activities are also determined by the way the Controller uses the Software and the AI Providers the Controller configures within it. Atelyr maintains a record of processing activities in accordance with Article 30(2) GDPR.