

Privacy Policy

Version 1 - Effective date 1st of May 2026

Atelyr B.V. ("Atelyr", "we", "us", "our") attaches great importance to the protection of your personal data. In this Privacy Policy, we explain what data we collect, why we do so, how we protect it, and what rights you have. This policy applies when you:

- visit our website at www.atelyr.ai or any other website that refers to this Privacy Policy ("Website"); or
- use our platform or applications ("Software"); or
- use the partner portal as a Partner ("Partner Portal"); or
- contact us by email, chat, or any other means.

This Privacy Policy has been drawn up in accordance with the General Data Protection Regulation (GDPR), which applies throughout the European Union.

Definitions

- **Data Subject:** the natural person to whom personal data relates, including End Customers, employees of Partners, and End Users.
- **End User:** the natural person who, through the Software, interacts with an AI agent deployed by an End Customer, 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. With respect to End User data, Atelyr acts as a processor, on behalf of the End Customer.
- **End Customer:** the natural person or legal entity that purchases the Software, either directly from Atelyr or through a Partner. The End Customer is the controller with respect to the personal data of End Users processed through the Software.
- **User:** the natural person who, on behalf of an End Customer or Partner, has access to the Software or the Partner Portal, such as an employee or freelancer. The End Customer or Partner is the controller with respect to the personal data of its Users. With respect to this data, Atelyr acts as a processor.
- **Partner:** a reseller who offers the Software to End Customers through Atelyr's partner or affiliate channel, and who receives a commission for End Customers it introduces. The Partner is itself responsible for compliance with applicable laws and regulations towards its End Customers.

ATELYR

1. Controller

The controller within the meaning of the GDPR is:

Atelyr B.V.

Dorpsstraat 324A, 1531 HW Wormer, Netherlands

Chamber of Commerce number: 99674327

Email: privacy@atelyr.ai

Website: www.atelyr.ai

Atelyr has appointed a Data Protection Officer (DPO). The DPO supervises compliance with the GDPR within Atelyr and is the primary point of contact for privacy-related questions. The DPO can be reached at:

Data Protection Officer

Email: dpo@atelyr.ai

Post: Atelyr B.V., Attn. Data Protection Officer, Dorpsstraat 324A, 1531 HW Wormer, Netherlands

In accordance with Article 38(4) GDPR, the Data Protection Officer is available to all data subjects, including End Customers, Partners, and their employees, who have questions about the processing of their personal data by Atelyr or about the exercise of their rights. Data subjects may contact the DPO directly at dpo@atelyr.ai, without the need for involvement from any other department. The DPO acts independently and is bound by confidentiality.

2. What Personal Data Do We Process?

2.1 Data you provide yourself

Atelyr collects personal data that you voluntarily provide when you:

- create or manage an account
- accept the applicable terms
- use the Software or the Partner Portal
- sign up for commercial communications such as the newsletter
- contact Atelyr by phone, chat, email, or any other means

The personal data we collect in this context includes:

- Name (first and last name)
- Email address
- Telephone number
- Company name and address
- VAT number
- Business registration number

ATELYR

- Job title
- Username and encrypted password

When accepting the applicable terms, Atelyr also records the following as evidence of consent:

- IP address and device data
- Browser and operating system information
- Date and time of acceptance

If an End Customer or Partner grants employees or other Users access to the Software or the Partner Portal, Atelyr processes the personal data of those Users solely on behalf of and for the benefit of the relevant End Customer or Partner. The End Customer or Partner is responsible for informing its Users about the processing of their personal data and for obtaining a valid legal basis for such processing.

2.2 Automatically collected data

When you use the Website, the Software, or the Partner Portal, Atelyr automatically collects the following data:

- IP address and device data
- Browser and operating system information
- Date and time of interactions
- Usage statistics (such as minutes consumed, features used, session data, configuration settings, and performance data of the AI agent)
- Log files and error messages

For the use of cookies, please refer to Article 9 and the Cookie Policy.

2.3 Payment data

Payments are processed via a certified payment provider. Atelyr does not store full payment details. Atelyr only processes:

- Billing address
- Payment history and invoice data

2.4 Conversation and metadata of AI agent interactions

In the context of the AI agent services, Atelyr processes the following data on behalf of its customers ("End User data"):

- Audio recordings of conversations conducted through the Software
- Transcripts or summaries generated by AI

- Metadata of interactions (date, duration, participants, and channel-specific identifiers such as the caller's phone number or a session ID)
- Personal data spoken or written during interactions

Atelyr processes this data solely as a processor within the meaning of the GDPR, on behalf of and for the benefit of the customer (End Customer) deploying the voice agent. The customer is the controller with respect to the callers whose data is processed, and is itself responsible for informing those callers about the processing of their personal data. The content of conversations is not used for commercial purposes or profiling. Atelyr has no control over what the AI provider chosen by the customer does with the data.

2.5 Data from incoming contact requests and communications

When you contact Atelyr, or when Atelyr contacts you by phone, chat, email, or any other means, Atelyr processes the following data:

- Telephone number, email address, or other contact details
- Content of the conversation, chat, or email message
- Metadata of the contact (date, time, duration, channel)
- Outcome of the conversation or follow-up actions

For the handling of contacts by phone, chat, or email, Atelyr may make use of automated AI agents. Atelyr informs data subjects at the beginning of each conversation or chat that they are communicating with an AI agent.

2.6 Sensitive data

The Software is not intended for the processing of sensitive personal data, such as data about health, religion, political opinions, or trade union membership. We do not ask for this kind of data and we do not use it for our own purposes.

In practice, End Users may sometimes share sensitive data during a conversation with an AI agent, for example by mentioning a health issue when calling customer service. Where this happens, Atelyr processes that data only as a processor, on behalf of the End Customer, in line with Article 2.4.

If an End Customer expects sensitive data to come up regularly in conversations with its AI agent, the End Customer is responsible for making sure it has a valid legal ground for processing such data and for informing End Users about it.

Atelyr does not use voice recordings to identify individuals based on the unique characteristics of their voice.

3. Purposes and Legal Bases

3.1 Purposes of processing

Atelyr processes your personal data for the following purposes:

- Creating and managing your account (*performance of contract*)
- Providing and maintaining the Software and the Partner Portal (*performance of contract*)
- Processing payments and invoices (*performance of contract*)
- Conducting onboarding and providing training and documentation (*performance of contract*)
- Entering into, managing, and recording agreements with Partners, End Customers, and suppliers, including partner agreements, license agreements, data processing agreements, and the acceptance of applicable terms (*performance of contract and legal obligation*)
- Handling incoming contact requests and providing customer service (*performance of contract or pre-contractual measures at the data subject's request; for other contacts: legitimate interest, see Article 3.5*)
- Sending administrative and transactional messages, such as updates to terms, usage notifications, limits, outages, and product updates (*performance of contract*)
- Sending commercial communications, in accordance with your preferences; you may unsubscribe at any time (*consent*)
- Managing partner relationships, including registering and following up on customers introduced via Partners (*performance of contract*)
- Account management and lead management, including customer segmentation for targeted service delivery (*legitimate interest, see Article 3.5*)
- Improving the Software based on anonymized usage data (*legitimate interest, see Article 3.3*)
- Ensuring the security and integrity of the Software, including fraud prevention (*legitimate interest, see Article 3.4*)
- Complying with legal obligations, such as tax retention requirements (*legal obligation*)

3.2 Legal bases for processing

Atelyr processes personal data only on the basis of a valid GDPR legal ground:

- **Consent:** you have expressly given consent for a specific processing activity, such as receiving commercial communications. You may withdraw your consent at any time.
- **Performance of a contract:** the processing is necessary for the performance of a contract with you, or for taking pre-contractual measures at your request.
- **Legal obligation:** the processing is necessary to comply with a legal obligation, such as tax retention obligations or obligations under Article 28 GDPR.
- **Legitimate interest:** the processing is necessary for the legitimate interests of Atelyr, provided that these do not outweigh your rights and freedoms. See Articles 3.3 to 3.5 for further clarification. On the basis of Article 8.1, you may object at any time to processing based on legitimate interest.

To the extent that Atelyr processes personal data on behalf of its End Customers and Partners in the context of the services purchased by them, Atelyr acts as a processor within the meaning of Article 28 GDPR and acts solely on the instructions of the End Customer or Partner as controller.

3.3 Legitimate interest: improvement of the Software

Interest of Atelyr: improving the quality, stability, and user-friendliness of the Software for the benefit of all users.

Nature of processing: exclusively anonymized or aggregated usage data, such as the number of sessions, error messages, and duration of use. Conversation content, audio, or directly identifiable data are not processed for this purpose.

Reasonable expectations of data subjects: users of software platforms may reasonably expect that anonymized usage data is used for product development. This is a common and recognizable practice.

Outcome of the balancing test: given the limited privacy impact (no identifiable data, no profiling) and the legitimate purpose, Atelyr's interest outweighs the interests of data subjects.

3.4 Legitimate interest: security and fraud prevention

Interest of Atelyr: safeguarding the integrity, availability, and security of the Software and the underlying systems, as well as preventing misuse and fraud.

Nature of processing: technical data such as log files, IP addresses, and access data. This data is processed solely for security purposes and not for profiling or other purposes.

Reasonable expectations of data subjects: users of digital services may reasonably expect a provider to take technical measures to ensure the security of the platform. This is a generally recognized and necessary practice.

Outcome of the balancing test: given the legitimate and necessary nature of security processing, the limited privacy impact, and the reasonable expectations of data subjects, Atelyr's interest outweighs the interests of data subjects.

3.5 Legitimate interest: account management, lead management, and other contact requests

Interest of Atelyr: being able to manage customer relationships and leads for the purpose of targeted service delivery, as well as handling incoming contact requests from persons who are not (prospective) customers or partners.

Nature of processing: contact details and account information, processed solely for the management of the relationship or the handling of the relevant request. In the case of contact requests, the data subject takes the initiative.

Reasonable expectations of data subjects: users of a business platform may reasonably expect that their account data is used for the management of the service. A person who contacts us of their own accord may reasonably expect that their data is processed for the handling thereof.

Outcome of the balancing test: given the minimal privacy impact, the legitimate purpose, and the reasonable expectations of data subjects, Atelyr's interest outweighs the interests of data subjects.

On the basis of Article 8.1, data subjects may object at any time to processing based on legitimate interest.

4. Retention Periods

4.1 Atelyr does not retain personal data longer than necessary for the purposes for which it was collected, or for as long as legally required. If a legal obligation requires a longer retention period than stated below, that legal obligation prevails.

4.2 The following retention periods apply:

- **Data you provide yourself, including identification and contact data** (Article 2.1): for the duration of the Agreement, plus 1 year after termination. For contracts, agreements, and evidence of acceptance of terms, a retention period of 5 years after termination applies, for the purpose of legal evidence within the applicable limitation periods.
- **Automatically collected data and log files** (Article 2.2): a maximum of 12 months, with the exception of usage statistics, for which a retention period of a maximum of 3 years applies.
- **Payment data and invoices** (Article 2.3): 7 years (statutory retention obligation under tax legislation).
- **Conversation and metadata of AI agent interactions** (Article 2.4): a maximum of 90 days after the conversation, unless one of the following grounds applies:
 - Performance of the contract: if longer retention is necessary for an ongoing dispute, complaint, or support request, for the duration of the handling thereof.
 - Consent of the End Customer: if the End Customer has expressly consented to longer retention, for as long as the consent applies. Consent may be withdrawn at any time, after which the data will be deleted within 30 days.
- **Data from contact requests and communications** (Article 2.5): for the duration of the Agreement and up to 1 year after its termination, or up to 2 years after the last contact, whichever is the longer period.
- **Commercial communications**: until withdrawal of consent, after which the data will no longer be used for commercial communications.

4.3 After expiration of the retention period, personal data is securely deleted or anonymized. Where possible, Atelyr uses automated processes without human intervention. Data subjects do not receive separate notification of routine deletion or anonymization. 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.

5. Sharing of Personal Data with Third Parties

5.1 Atelyr only shares personal data with third parties if this is necessary for the provision of services, legally required, or if the data subject has consented to it.

5.2 Atelyr uses the following categories of processors and recipients:

- **Payment providers:** for the processing of payments and invoice data.
- **Hosting parties:** for the storage of data on secure servers within the EU, including identification and contact data, usage data, and log files.
- **Email providers:** for sending invoices, service notifications, and commercial communications.
- **AI providers for product functionality:** for generative AI features within the Software, including the processing of conversation content, the optimization of prompts, and the building of knowledge bases (RAG). This may involve the processing of both End User data and data entered into the Software.
- **Communication and collaboration platforms:** for internal and external communications, document storage, and meetings, including email, documents, and video conferencing.
- **Communication and support platforms:** for the handling of incoming contact requests and customer service by phone, chat, or email, including via automated AI agents.
- **Financial administration solutions:** for bookkeeping and financial administration, including invoice data and payment history.
- **Monitoring and logging providers:** for monitoring system performance, log management, and incident management for the security of the Software.
- **Accountants, lawyers, and tax advisors:** for compliance with legal obligations.

5.3 With all processors that process personal data on behalf of Atelyr, Atelyr concludes a data processing agreement that meets the requirements of the GDPR.

For AI providers that the End Customer independently selects within the Software, Atelyr acts as a contracting party and concludes a data processing agreement with the chosen AI provider on behalf of the End Customer. By making this explicit choice, the End Customer assumes all responsibilities arising from the processing by that provider.

5.4 Atelyr never sells personal data to third parties.

5.5 An up-to-date overview of the processors engaged by Atelyr is available via docs.atelyr.ai. This overview is updated regularly.

6. Transfer of Personal Data Outside the EU

6.1 Atelyr transfers personal data outside the European Economic Area (EEA) only to the extent necessary for the provision of services. Transfers may take place via processors engaged by Atelyr, such as hosting parties, AI providers for product functionality, monitoring and logging providers, and email providers.

ATELYR

Transfers may also take place because End Customers themselves select and configure an AI provider established outside the EEA, including in the United States.

To the extent that End User data is processed via processors selected and configured by Atelyr, Atelyr ensures that such processing takes place exclusively within the EEA. This does not apply to processing via AI providers that the End Customer selects itself; for those, the provisions of Article 6.3 apply.

6.2 Atelyr ensures that transfers outside the EEA only take place on the basis of one of the following appropriate safeguards:

- 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; or
- 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 recognized by the GDPR, including the derogations for occasional transfers.

6.3 If the End Customer 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 End Customer, including the applicable transfer safeguards. The End Customer decides how that provider processes the data and acts as controller. The detailed contractual arrangements are set out in the applicable Data Processing Agreement.

Atelyr only facilitates the technical connection and has no control over, or insight into, the processing activities performed by the AI provider.

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

7. Security

7.1 Atelyr takes appropriate technical and organizational measures to protect personal data against loss, unauthorized access, disclosure, or destruction.

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

- Encryption of data
- Access control and authentication
- Monitoring and logging
- Backup and recovery
- Periodic security audits
- Incident management
- 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.

7.3 In its data processing agreements, Atelyr stipulates that processors take equivalent security measures.

For AI providers selected by the End Customer, Atelyr presents the security and compliance information disclosed by each provider (such as certifications, data residency, and GDPR status), so that the End Customer can make an informed choice based on its own requirements. Atelyr accepts the data processing agreement and security terms offered by the chosen provider on the End Customer's behalf. The End Customer remains responsible for selecting a provider that meets its own security and compliance needs.

7.4 Where Atelyr acts as controller (in particular for the data described in Articles 2.1–2.3 and 2.5), Atelyr will report any data breach likely to pose a risk to data subjects to the Dutch Data Protection Authority, without undue delay and where possible within 72 hours of becoming aware of it. If the breach entails a high risk, data subjects will be informed directly without undue delay. Atelyr records all data breaches internally, regardless of whether reporting is required.

7.5 Where Atelyr acts as processor (in particular for the End User data described in Article 2.4), Atelyr will notify the relevant End Customer of any data breach without undue delay. The End Customer, as controller, is responsible for any further notifications to the supervisory authority and to data subjects.

8. Your Rights as a Data Subject

8.1 Under applicable privacy legislation, you have the following rights with regard to your personal data:

- **Right of access:** you have the right to know what personal data Atelyr processes about you.
- **Right to rectification:** you have the right to have incorrect or incomplete data corrected.
- **Right to erasure:** you may request the deletion of your data, unless Atelyr has a legal or contractual obligation to retain it, or another legal basis for processing applies.
- **Right to restriction of processing:** you may have the processing of your data restricted in certain cases.
- **Right to data portability:** you have the right to receive your data in a structured, commonly used, and machine-readable format.
- **Right to object:** you may object to processing based on Atelyr's legitimate interest.
- **Right to withdraw consent:** if processing is based on consent, you may withdraw it at any time without affecting the lawfulness of processing carried out before the withdrawal.

8.2 The rights listed above are not absolute. In certain cases, Atelyr may refuse a request in whole or in part, for example if granting the request would conflict with a legal obligation or the rights of third parties.

8.3 You may exercise your rights by sending a request to privacy@atelyr.ai. To verify your identity, Atelyr may ask you to provide additional information. Atelyr will respond to your request within one month. In the

case of complex or multiple requests, this period may be extended by two months, of which Atelyr will inform you in a timely manner.

8.4 You have the right to lodge a complaint with the privacy supervisory authority in your country if you believe that Atelyr is not processing your personal data in accordance with the GDPR. An overview of the competent supervisory authorities within the European Union is available at edpb.europa.eu.

9. Cookies and Tracking Technologies

9.1 Atelyr uses cookies and similar technologies on the Website and in the Software. Functional cookies are necessary for the functioning of the Website and are placed without consent. For analytical and marketing cookies, Atelyr requests your consent in advance via a cookie banner. You may withdraw your consent at any time as described in the Cookie Policy.

9.2 A complete overview of the cookies used and their purposes is available in the Cookie Policy on the Website.

10. Changes to this Privacy Policy

10.1 Atelyr reserves the right to amend this Privacy Policy. Amendments will be published on the Website and will take effect from the date of publication.

10.2 The date of the most recent amendment is indicated at the top of this document.

11. Automated Decision-Making and Profiling

11.1 Atelyr does not use 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.

11.2 The Software uses artificial intelligence (AI) for various functionalities, including the processing of conversation content and the generation of prompts. This technology is used solely as a supporting tool for the provision of services. Outcomes generated by AI do not form the basis for automated decisions with legal effects and are not used for profiling of data subjects.

If an End Customer's setup leads to decisions that significantly affect data subjects, the End Customer is responsible for complying with the relevant rules, including providing meaningful information about how the decision is made, allowing human review on request, and giving the data subject a right to challenge the decision.

12. Minors

12.1 Atelyr's Software and Website are not intended for persons under the age of 16. Atelyr does not knowingly process personal data of minors.

12.2 If Atelyr becomes aware that personal data of a person under the age of 16 has been collected without a valid legal basis, Atelyr will delete this data as soon as possible.

12.3 Partners and End Customers that deploy the Software in a context where minors may be involved are themselves responsible for obtaining the required consent of the parent or legal representative, and for compliance with the applicable laws and regulations for the protection of minors. Atelyr is not liable for the processing of personal data of minors resulting from the use of the Software by Partners or End Customers.

13. Contact

For questions, comments, or requests regarding this Privacy Policy or the processing of your personal data, you may contact:

Atelyr B.V.

Dorpsstraat 324A, 1531 HW Wormer, Netherlands

Email: privacy@atelyr.ai

Website: www.atelyr.ai