



Privacy Policy

Repetitive B.V., trading as Repetitive, Spoorlaan 181, 5038 CB Tilburg, the Netherlands (Chamber of Commerce / KvK: 99365421), is the controller responsible for your personal data as described in this policy.

Version: 2.2

Last updated: 5 October 2026

Document owner: Chief Information Security Officer

Review cycle: annually, or earlier when our processing activities change

Introduction

This privacy policy describes how we collect and use your personal data when you visit our website, contact us, do business with us, or apply for a job with us. It also explains your rights and how to exercise them.

This policy covers the personal data for which Repetitive is the **controller**. When we build and operate AI agents for our business customers, we process personal data on their behalf and act as a **processor** under a separate Data Processing Agreement (DPA), not under this privacy policy. If your data is processed through a Repetitive agent operated for one of our customers, that customer is the controller and their privacy policy applies. An up-to-date overview of the sub-processors we use in that processor role is available in our Trust Center at <https://www.repetitive.ai/trust-center>.

Who this policy applies to

This policy applies to:

- visitors of our website;
- prospects and business contacts of (potential) customers and partners;
- contact persons at our customers who interact with us directly (for example by email or in meetings);
- job applicants.

What personal data we collect

Contact and business communications. When you contact us by email or phone, or when we meet, we process your name, business contact details and the content of our communication.

Business contact information. We keep contact details of prospects, customers and partners (name, business email address, phone number, organisation, role, and notes on our interactions) in our CRM system (Odoo).

Data we do not collect from you directly. We may also obtain business contact details from publicly available online sources, such as professional networking profiles (for example LinkedIn), company

websites and the Dutch trade register (KvK), and from commercial providers of business contact databases (such as Apollo). Where we do, we only collect standard business contact details (name, role, organisation, business contact details) and we inform you of this processing no later than at our first communication with you, in accordance with Article 14 GDPR.

Job applications. When you apply for a job, we collect the information you provide, such as your name, contact details, CV, motivation letter and any other information you share during the application process.

Usage information. When you visit our website, we may collect log data, device information and approximate location information, subject to applicable law and, where required, your consent (see the Cookies section).

Why we use your personal data and on which legal basis

Purpose	Examples	Legal basis (Art. 6 GDPR)
Providing our services	Delivering our services to our customers, customer support, communicating with you as a contact person for your organisation	Performance of a contract (6(1)(b)); legitimate interest (6(1)(f)) where you act as a contact person for your organisation
Sales, relationship management and direct marketing	Responding to inquiries, maintaining our CRM, contacting prospects and customers about our services	Legitimate interest (6(1)(f)): running and growing our business through direct B2B contact; you can object at any time
Improving our services and website	Analysing how our website is used (Google Analytics, Microsoft Clarity), gathering feedback	Consent (6(1)(a)) for analytics cookies; legitimate interest (6(1)(f)) for feedback you provide to us
Security and fraud prevention	Detecting and preventing abuse and security incidents, access logging	Legitimate interest (6(1)(f)): keeping our services and data secure
Recruitment	Assessing your job application and communicating with you during the process	Legitimate interest (6(1)(f)): recruiting staff; consent (6(1)(a)) for retaining your data beyond the procedure
Legal compliance	Financial administration, responding to lawful requests from authorities	Legal obligation (6(1)(c))

You are generally not obliged to provide us with your personal data. However, without certain data (such as your name and email address) we cannot provide our services, respond to your inquiry or process your application.

Our use of AI tools

We use AI tools (large language models) to support our internal processes, such as handling email and administration. Where these tools process personal data, we exclusively use Google Vertex AI, hosted within the European Union: the provider does not retain the personal data we submit, and your personal data is not used to train AI models. For internal operational tasks that do not involve personal data, we may also use other AI providers (such as Anthropic).

When we operate AI agents for our customers (in our role as processor), AI model inference also runs on Google Vertex AI within the European Union, without retention of the data submitted; see our Trust Center for details.

Where our communication with you is drafted or generated with the help of AI, it is reviewed by a person before it is sent. Where required under the EU AI Act, we will make clear when you are interacting with an AI system or when content has been generated by AI.

Automated decision-making

We do not make decisions based solely on automated processing, including profiling, that produce legal effects concerning you or that similarly significantly affect you (Article 22 GDPR). AI tools may support our work, but decisions that affect you (for example about your job application) are always made by a person.

Who we share personal data with

Service providers (processors). Third parties that provide services on our behalf may process personal data as instructed by us. These include Google Workspace / Google Cloud (email, documents, hosting, AI via Vertex AI, website analytics via Google Analytics), Microsoft (website analytics via Clarity), Notion (knowledge base and internal documentation), Cloudflare (website security and performance) and Odoo (CRM and business administration). We have data processing agreements in place with these providers.

Professional advisors. Personal data may be disclosed to professional advisors such as lawyers, accountants and auditors, where necessary for the services they provide to us.

Authorities. We may disclose personal data to law enforcement or government authorities where we are legally required to do so, or where necessary to protect rights, safety or property and to enforce our terms.

Business changes. In the event of a merger, acquisition or similar business change, personal data may be transferred subject to appropriate confidentiality arrangements.

We never sell your personal data.

Transfers outside the EEA

We primarily use service providers that process personal data within the European Economic Area (EEA). Where personal data is transferred outside the EEA, we rely on an appropriate transfer mechanism under the GDPR, such as an adequacy decision, the EU Standard Contractual Clauses (SCCs) or the EU-U.S. Data Privacy Framework (DPF). Data collected via Microsoft Clarity and Google Analytics, and the business contact details and meeting notes in our knowledge base in Notion, may be stored by Microsoft, Google and Notion on servers outside the EEA; Microsoft, Google LLC and Notion Labs, Inc. are certified under the EU-U.S. Data Privacy Framework. You can request a copy of the relevant safeguards via privacy@repetitive.ai.

How long we keep personal data

Category	Retention period
Customer and contract-related data	Duration of the contract, plus 2 years after the end of the contract
CRM data of prospects and business contacts	2 years after our last meaningful contact
Contracts and financial administration	7 years (Dutch statutory retention obligation)
Job application data	Deleted within 4 weeks after the end of the application procedure, or up to 1 year with your consent
Security and access logs	12 months

When we no longer need your personal data, we delete or anonymise it. If immediate deletion is not possible (for example because the data is stored in backup archives), we securely store it, isolate it from further processing, and delete it when the backup cycle allows.

Data security

We use up-to-date industry standards and practices to protect personal data against loss, misuse and unauthorised access or disclosure, taking into account the sensitivity of the data and the state of technology. We also require the service providers with whom we share personal data to implement appropriate security measures. No transmission or storage system can be guaranteed to be completely secure; if a data breach occurs that is likely to result in a risk to your rights, we will inform the Dutch Data Protection Authority and, where required, you.

Cookies

We only place cookies that are not strictly necessary after you have given your consent via our cookie banner. You can withdraw your consent at any time via your cookie settings.

Cookie category	Purpose / examples	Consent
Necessary / functional	Required for the website to work (security, load balancing via Cloudflare, remembering your cookie choices)	Placed without consent
Analytics / session insights	Google Analytics: aggregated website statistics. Microsoft Clarity: behavioural metrics, heatmaps and session replay to improve our website	Placed only after consent

With your consent, we use **Google Analytics** to measure how our website is used (pages visited, traffic sources, aggregated visitor statistics) and **Microsoft Clarity** to understand how visitors use our website. Clarity is configured so that text entered by users (such as form fields) and images are masked by default and are not visible in session recordings. This data is processed by Google and Microsoft, which may store it on servers outside the EEA under the EU-U.S. Data Privacy Framework (see Transfers outside the EEA). For more information, see the Google Privacy Policy at <https://policies.google.com/privacy> and the Microsoft Privacy Statement at <https://www.microsoft.com/privacy/privacystatement>.

If you prefer not to have cookies stored on your device, you can reject non-necessary cookies via our cookie banner, adjust your browser settings, or remove cookies manually. Rejecting cookies may limit some functionality of our website. To learn more about cookies, visit www.allaboutcookies.org.

Links to other websites

Our website may contain links to other websites. This privacy policy does not cover the practices of third parties. We recommend reading the privacy policy of any website you visit before providing personal data.

Children

Our website and services are directed at businesses and are not intended for children under 16. We do not knowingly collect personal data from children under 16. If you believe we have done so, please contact privacy@repetive.ai and we will delete the data.

Your rights

You have the right to:

- be informed about the personal data we process about you;
- access the personal data we process about you;
- rectify or update your personal data;
- request the deletion of your personal data;
- request the restriction of the processing of your personal data;
- object to certain uses of your personal data, including direct marketing;
- withdraw your consent at any time, without affecting the lawfulness of processing before withdrawal;
- data portability.

To exercise these rights, contact us at privacy@repetive.ai. We may ask you to verify your identity first. We will respond within one month.

If your personal data is processed through an AI agent that we operate for one of our customers, that customer is the controller. Please contact them directly; we will assist them in fulfilling your request.

If you believe your rights have been violated, you can lodge a complaint with the Dutch Data Protection Authority (Autoriteit Persoonsgegevens, www.autoriteitpersoonsgegevens.nl) or with the supervisory authority in your own EU member state.

Marketing

If you no longer wish to receive emails from us about our services, you can let us know at any time by replying to the email or by contacting privacy@repetive.ai. We will then stop contacting you for marketing purposes.

Contact

For questions or concerns about this privacy policy or our data protection practices, contact our privacy contact (the Chief Information Security Officer):

Email: privacy@repetive.ai

Changes to this privacy policy

We update this privacy policy from time to time. When we do, we will update the "Last updated" date above and post a notice on this page. For material changes, we may also notify you by email.