

Velonos

Terms of Service

1. The Provider is the creator, owner and entity entitled to make available the “Velonos” application (the “Application”), whose function is to protect Sensitive Information (as defined below) processed by users while using external artificial intelligence tools, including in particular ChatGPT (OpenAI), Claude (Anthropic) and Gemini (Google) (collectively, the “AI Providers”), by detecting Sensitive Information on the user’s device and replacing it with tokens before a prompt or attachment is sent to an AI Provider, and then, after receiving the response, restoring the original data in place of the tokens (all these operations are performed locally on the user’s device);
2. The Provider and the Client are hereinafter jointly referred to as the “Parties” and individually as a “Party”.
3. These Terms of Service (“Terms”) constitute, in particular, a license agreement under which the Supplier grants the Customer a non-exclusive licence to use the Application (§ 4), and further set out the rules on: deployment and technical support, the commercial terms governing the provision of Application, personal data protection, confidentiality and security measures, the Parties’ liability, and the term and termination of the Agreement.

§ 1. DEFINITIONS

Terms capitalized in these Terms of Service (“Terms”) have the following meanings:

1. “Provider” means Software Mansion S.A., with its registered office at ul. Zabłocie 43B, 30-701 Kraków, Poland, entered in the Register of Entrepreneurs of the National Court Register maintained by the District Court for Kraków-Śródmieście in Kraków, 11th Commercial Division of the National Court Register, under KRS No. 0000961952, Tax Identification Number (NIP) 6793131302, REGON 364909814.
2. “Application” means the software provided by the Provider under the name “Velonos”, together with the Detection Model, whose function is to detect Sensitive Information in prompts and attachments submitted by Users to AI Providers, replace it with Tokens before transmission, and then restore the original content in the response received from the AI Provider;
3. “Detection Model” or “Model” means the Provider’s proprietary artificial intelligence model, developed and trained by the Provider and used by the Application to detect Sensitive Information; the Detection Model operates locally on the User’s Device;
4. “Sensitive Information” means data designated by the Client or detected by default by the Detection Model as requiring protection, including in particular personal data within the meaning of Article 4(1) of the GDPR, special categories of personal data within the meaning of Article 9 of the GDPR, the Client’s trade secrets, data covered by professional secrecy, or other confidential information listed in Appendix 1;
5. “Token” means a technical text symbol used by the Application to replace detected Sensitive Information before content is transmitted to an AI Provider, enabling the original content to be restored later;
6. “User’s Device” means a computer or other end-user device on which the Application is installed and run;
7. “User” means an employee, associate or other person authorized by the Client to use the Application under a Seat assigned to them;

8. “Seat” (Licence) means a single access seat for the Application assigned to one User;
9. “AI Providers” means external providers of artificial intelligence tools used by the Client through the Application, including OpenAI (ChatGPT), Anthropic (Claude) and Google (Gemini), as well as other providers agreed by the Parties; AI Providers are not parties to these Terms, and the Client’s relationship with each AI Provider is governed by separate agreements entered into directly between the Client and that AI Provider;
10. “Activity Log” means a local event log recorded by the Application on the User’s Device, recording activity related to use of the Application to the extent and on the terms described in § 7 of these Terms;
11. “Token Database” means a local collection stored on the User’s Device containing original Sensitive Information together with its assigned Tokens, used by the Application to restore the original content in responses from AI Providers;
12. “GDPR” means 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;

Unless the Terms provide otherwise, “days” means calendar days.

§ 2. SCOPE OF SERVICE

1. The subject of these Terms is the provision of the Application by the Provider to the Client, together with its implementation within the Client’s organization, on the terms and within the scope set out in these Terms.
2. Under the Terms, the Provider undertakes in particular to: (a) make the agreed number of Seats available to the Client; (b) ensure that the Application operates in accordance with its intended purpose described in the preamble and Appendix 1 (Functional Specification); (c) support implementation of the Application in the Client’s organization through a dedicated communication channel on the terms described in these Terms, and (d) provide technical support on the terms described in these Terms.
3. At the Client’s separate request, the Provider may fine-tune the Detection Model to the specifics of the Client’s business using sample documents provided by the Client (the “Fine-Tuning Service”). The terms governing the Fine-Tuning Service, including the use and confidentiality of documents provided by the Client, are set out in a separate order/amendment to these Terms. The Fine-Tuning Service is not a part of the general Velonos scope of Service without the Client’s choice to use it.
4. The Parties confirm that the Application is not a party to, nor an intermediary under, any licence agreements or terms governing the Client’s relationship with AI Providers. The Client’s use of ChatGPT, Claude, Gemini or other AI tools is governed by separate agreements/terms entered into directly between the Client and the relevant AI Provider, for whose content and performance the Application Provider accepts no responsibility.

§ 3. COMMERCIAL TERMS

1. By accepting these Terms, the Parties shall enter into a Commercial Agreement on the terms set out herein. The Commercial Agreement shall be concluded as a renewable subscription, for a monthly or annual term, at the Client’s choice.
2. The licence fee is available under the link velonos.ai/#pricing, and payable in advance against a VAT invoice issued monthly by the Provider, based on the number of active Seats assigned to the Client on the first day of the relevant billing period. The payment term is 15 days from delivery of a correctly issued invoice. The number of Seats may be increased or decreased during the term of the Commercial Agreement in accordance with the terms set forth under the link []; the change shall take

effect immediately, with the charge adjusted pro rata on the nearest invoice. Before confirming the change, the Customer shall be shown the modified rate.

3. The fee referred to in subclause 2 may be changed by the Provider subject to at least 60 days' prior written notice to the Client. In that case, the Client may refuse to accept the change and not renew the Commercial Agreement.

4. If payment is more than 14 days overdue, the Provider may, after issuing an unsuccessful payment demand allowing an additional 7-day period for payment, suspend access to the Application until the arrears are paid, without prejudice to the Provider's other rights, including the right to terminate the relationship between Parties.

5. The subscription shall renew automatically for a further term of the same length as the preceding one, unless the Client cancels it before the end of the then-current term.

6. The Client may cancel the subscription at any time through the feature available in the console or in the Application (depending on the account type). Cancellation takes effect at the end of the then-current term, and the Client retains access to the services until that date.

7. A Client who is a consumer (understood as a natural person concluding the agreement for purposes not directly connected with their business or professional activity) may withdraw from the Commercial Agreement within 14 days of its conclusion by sending an unambiguous statement to hello@velonos.ai. By confirming the order, the Client expressly requests that the services begin immediately and acknowledges that, once the services have been fully performed, the right of withdrawal is lost. If the Client withdraws after performance has begun, the Client shall pay a proportionate amount for the services provided until the withdrawal, and the Provider shall refund the remainder within 14 days.

8. Except as provided in subclause 7 above or required by mandatory law, fees paid for a term that has begun are non-refundable, and cancellation under subclause 6 above applies only to subsequent terms.

§ 4. LICENSE AND INTELLECTUAL PROPERTY RIGHTS

1. For the term of these Terms, the Provider grants the Client a non-exclusive, non-transferable license (subject to § 10(4)) with no territorial limitation to use the Application through Users, in a number corresponding to the Seats granted, solely for the Client's internal business purposes.

2. The license does not include the right to: (a) make the Application available to third parties outside the Client's organization or sublicense it; (b) decompile, disassemble or reverse engineer the Application or Detection Model, except where mandatorily permitted by law; or (c) remove or modify the Provider's intellectual property notices.

3. All intellectual property rights in the Application, Detection Model and any modifications, improvements and developments thereof, remain the exclusive property of the Provider. The Terms transfer no intellectual property rights to the Client other than the license described in section 1.

4. The Client retains all rights to any data entered into the Application by Users, including data contained in prompts, attachments, the Token Database and the Activity Log.

§ 5. PERSONAL DATA PROTECTION

1. The Parties acknowledge that use of the Application may involve processing personal data (within the meaning of Article 4(1) of the GDPR), including, given the nature of Sensitive Information, special categories of personal data within the meaning of Article 9 of the GDPR contained in prompts and attachments submitted by Users.

2. The Application's core operating principle is to modify data locally on the User's Device. The Provider represents that the Application has been designed using a "zero-access" architecture (no

Provider access to data), meaning that: (a) detection of Sensitive Information, its tokenization, storage in the Token Database, generation of the Activity Log and restoration of the original content all take place exclusively locally on the User's Device; (b) no data derived directly from prompt content, attachments, the Token Database or Activity Log, particularly through telemetry, error reporting, diagnostics or Application updates, is automatically transmitted, replicated or otherwise made available to the Provider or any third party; and (c) the Provider has no technical ability to remotely read, export or view the contents of the Client's Token Database or Activity Log. Appendix 1 contains a detailed description of the technical architecture confirming the above. Accordingly, within the scope described in this section, the Provider does not act as a processor within the meaning of Article 28 of the GDPR.

3. The Provider undertakes not to introduce into the Application any mechanism enabling remote Provider access to the contents of the Client's prompts, attachments, Token Database or Activity Log without the Client's prior written consent. Introducing such a mechanism, including as part of an Application update, requires prior notice to the Client.

6. The Parties confirm that data transmitted by the Application to AI Providers in tokenized form (i.e. without the original Sensitive Information) is transmitted under a separate contractual relationship between the Client and the relevant AI Provider. The Application Provider is not a party to that relationship, has no access to the content transmitted to AI Providers or to their responses, and accepts no responsibility for how AI Providers process data.

7. The Provider undertakes to apply appropriate technical and organizational measures to ensure the security of processed and stored data, proportionate to the risks associated with the nature of the Sensitive Information, as detailed in Appendix 1.

8. As controller of the personal data of Users and of persons whose data may be included in prompts or attachments, the Client is responsible for ensuring an appropriate legal basis for processing that data, including informing Users about the rules for using the Application and about the transmission of tokenized content to AI Providers.

§ 6. CONFIDENTIALITY

1. "Confidential Information" means all technical, technological, organizational, commercial and legal information disclosed by one Party to the other in connection with entering into or performing the Terms, including in particular these Terms and their appendices, Training Materials, data in the Activity Log and Token Database, information about the Client's Sensitive Information, and technical information concerning the operation of the Application and Detection Model, regardless of the form of disclosure and whether marked confidential.

2. Each Party shall keep the other Party's Confidential Information secret, shall not disclose it to third parties without the other Party's prior written consent, and shall use it solely to perform the Terms, except that Confidential Information may be disclosed: (a) to the Party's employees, associates and subcontractors bound by equivalent confidentiality obligations, to the extent necessary to perform the Terms; or (b) at the request of competent public authorities, to the extent required by law.

3. The confidentiality obligation does not apply to information that: (a) is or becomes publicly available without breach of these Terms; (b) was known to a Party before disclosure by the other Party; or (c) was independently developed by a Party without using the other Party's Confidential Information.

4. The confidentiality obligation applies during the term of these Terms and for 3 (three) years after its termination or expiry.

§ 7. SECURITY, ACTIVITY LOG AND TOKEN DATABASE

1. The Activity Log and Token Database are stored locally on the User's Device and, except are not transferred or made available to the Provider.
2. The Client (through its authorized administrators) may view, export and delete the contents of the Activity Log and Token Database using the functionality and in accordance with the rules described in Appendix 1.
3. The detailed scope of data recorded in the Activity Log (e.g. operation timestamps, types of detected Sensitive Information categories and diagnostic information) is specified in Appendix 1.
4. In each chosen moment the Client may export the Token Database and Activity or delete all the data stored in the Application through the relevant Application features.
5. The Provider shall inform the Client without undue delay, within the period prescribed by Polish law, upon identifying an Application security breach that may affect the Client's or Users' data.

§ 8. LIABILITY OF THE PARTIES

1. The Parties acknowledge that the Application is a tool intended to help reduce the risk of disclosure of Sensitive Information and does not guarantee that the Model will detect all Sensitive Information in every circumstance. The Client remains responsible for establishing and enforcing its internal policy on the use of AI tools within its organization and for final verification of content transmitted to AI Providers.
2. The Provider is liable for non-performance or improper performance of these Terms under the general rules of the Polish Civil Code, subject to the limitations below.
3. The Provider shall not be liable for the Client's loss of profits or indirect damage, unless the damage was caused intentionally by the Provider.
4. The liability limitations in this section do not apply to damage caused intentionally or to liability that cannot be limited or excluded under mandatory law (including the GDPR to the extent that the Provider acts as a processor).
5. Neither Party shall be liable for failure to perform its obligations under these Terms due to force majeure, understood as an external event independent of the Parties that could not have been foreseen or prevented.

§ 9. TERM AND TERMINATION

1. These Terms are concluded for an indefinite term.
2. Either Party may terminate the relationship with immediate effect in the event of: (a) a material breach of these Terms by the other Party that is not remedied within 14 days of receipt of a written notice (including by email); (b) breach by the other Party of confidentiality obligations (§ 5); or (c) declaration of bankruptcy, liquidation or commencement of restructuring proceedings in respect of the other Party.
3. Upon termination or expiry of these Terms, the Client's access to the Application shall be deactivated, without prejudice to the Client's rights to export data referred to in § 7(4). The provisions concerning confidentiality (§6), intellectual property (§ 4(4)), liability of the Parties (§ 8), and governing law and jurisdiction (§ 10) shall survive termination.

§ 10. FINAL PROVISIONS

1. Matters not governed by the Terms shall be subject to Polish law.

2. The Parties shall seek to resolve amicably any disputes arising out of or in connection with the Terms. If no agreement is reached, disputes shall be resolved by the common court having territorial jurisdiction over the Provider's registered office.
3. Any amendments to these Terms must be made in writing or in documentary form (including email confirmation), failing which they shall be null and void, except that Appendix 1 (Functional Specification) may be amended in documentary form as the Application is developed on an ongoing basis, provided that the functionality agreed by the Parties is not materially reduced.
4. Neither Party may transfer its rights or obligations under these Terms to a third party without the other Party's prior written consent, except that either Party may transfer these Terms to an entity within the same corporate group or to a purchaser of all or an organized part of its business, subject to prior notice to the other Party.
5. If any provision of these Terms is invalid or unenforceable, this shall not affect the validity of the remaining provisions. The Parties shall replace the invalid provision with one that most closely achieves its original commercial purpose.
6. The following appendices form an integral part of the Terms: Appendix 1 — Application Functional Specification and SLA terms.

APPENDIX 1

APPLICATION FUNCTIONAL SPECIFICATION AND SLA TERMS

1. Categories of Sensitive Information

1.1. Categories detected by default

Category	Types of Sensitive Information
Identity	full name; national identification number (i.e. NIN, PESEL); tax identification numbers (i.e. NIP, REGON); national ID card number; passport number; driving licence number; national identification number; tax identification number; US SSN; VIN and licence plate numbers; land and mortgage register number
Reference identifiers	employee number; customer number
Financial data	payment card number; IBAN / NRB; bank account number; SWIFT/BIC; cryptocurrency wallet address; wallet recovery phrase (seed); CVV/CVC/PIN
Contact details	email address; telephone number; postal address; internal hostname
Medical data	medical record number; health insurance number
Technical secrets	API key and access token; password; private key; JWT token; connection string; signed URL / webhook
Organization	company name
Network data	username; IP address
Location	GPS coordinates
Device	MAC address; device identifier
Dates	date of birth
Special categories of data (Article 9 GDPR)	religious beliefs; political opinions; sexual orientation; ethnic origin

1.2. Client configuration

Mechanism	Action
Enable / disable types	Each type in section 1.1 can be disabled
Exception list	Values that are never redacted (e.g. the Client's name)
Custom terms list	Client-specific phrases (e.g. project names), always redacted with their own token label

2. Supported AI Providers

AI Provider	Prompt content	Files transmitted	Restoration of data in response
ChatGPT (chatgpt.com)	yes	yes	yes
Claude (claude.ai)	yes	yes	yes

AI Provider	Prompt content	Files transmitted	Restoration of data in response
Gemini (gemini.google.com)	yes	yes	yes

The list may be expanded, and the Provider shall inform the Client each time it is expanded.

File formats	
Supported	TXT, CSV, MD, JSON, XML, PDF (including scans), DOCX, PPTX, images (PNG, JPG, GIF, WebP, HEIC, AVIF)
Blocked	XLSX, DOC, XLS, PPT, ZIP, email messages

3. Technical requirements for the User's Device

	macOS	Windows
Operating system	macOS 14 or later	Windows 10 / 11, 64-bit
Processor	Apple Silicon (M1 or later)	x64
RAM	min. 8 GB	min. 8 GB
Free disk space	min. 2 GB	min. 2 GB
Browser	Safari, Chrome, Edge, Firefox	Chrome, Edge, Firefox

4. Activity Log

Field	Description
Date and time	event timestamp (UTC)
AI Provider	service to which the request was sent
Status	redacted / no data to redact / blocked (prompt or file)
Detected categories	number of Sensitive Information items by type
Tokens	replacement tokens used in place of data
Reason for blocking	technical description, without data
Processing time	in milliseconds
Text size	number of characters in the prompt before redaction

The log is stored exclusively locally on the User's Device in JSON Lines format and does not contain original Sensitive Information values. The detailed event view in the Application (text before and after redaction) is stored locally only and is not transmitted to the Provider.

5. Availability parameters (SLA)

Component	Requires Provider infrastructure	If the Provider's infrastructure is unavailable
Detection, redaction, data restoration	no (operates locally)	unaffected
Application and Detection Model updates	yes (update server)	the installed version keeps working
Licence activation (sign-in with a work email or a licence key)	yes (console)	a new sign-in is not possible until the console answers
Licence verification (hourly check)	yes (console)	the Application keeps working on its last successful check for up to 7 days; after that, protection stops until the console answers
Organisation policy (shared redaction settings)	yes (console)	the Application keeps applying the last policy it received
Usage statistics (only when enabled by the Client)	yes (console)	reports wait and are sent after the next successful check

6. Updates

Area	Rule
Detection Model	updated together with the Application
Mechanism	automatic checking and downloading of cryptographically signed updates
Client notification	electronically, of every change to categories (section 1), AI Providers and formats (section 2), requirements (section 3) or Log scope (section 4), communicated to the Client in the release description in the legally mandated timeframe; security patches without delay