

Data Processing Agreement (DPA)

AI Presenter · version 2026-10-16 · prepared 16 October 2026 · effective upon recorded acceptance

This agreement under Article 28 GDPR is between the customer as controller and Sales Robots s.r.o., Company ID 09586563, Generála Šišky 2082/26, 143 00 Prague, info@salesrobots.cz, as processor. It forms part of the [Terms](#) and prevails on data protection matters. Sales Robots is an independent controller of account, billing and contract information under its [Privacy Policy](#). Electronic acceptance identifies the representative, company, time and exact document versions. Publication or acceptance of older, different terms does not replace it.

1. Instructions and responsibilities

Processing is solely on documented controller instructions within Appendix 1. Instructions include admin settings and written requests to info@salesrobots.cz: source materials, contact capture, optional consent wording, summary recipients, access and shorter retention. Functions not available in admin settings are handled through documented requests; this text does not declare new controls deployed. A new purpose or third-country transfer requires instructions unless EU or member state law requires it; we inform the controller beforehand unless legally prohibited. We promptly flag an unlawful instruction and defer it until clarified.

The controller determines purposes and legal bases and meets transparency and direct marketing duties. The processor supplies the information interface, a template and evidence; the controller is responsible for its notice and consent wording. Notice acknowledgement is not follow-up consent. Requested summaries must remain available without follow-up consent. None of this excludes the processor's own GDPR duties.

2. Confidentiality, security and no own-purpose use

Access is limited to authorised persons bound by confidentiality. The processor applies and reviews proportionate Article 32 safeguards in Appendix 2. The controller manages its users and instructions.

The processor does not use controller personal data or conversations for its own purposes, marketing, general model training or cross-client service improvement. Personal data is sent only to AI supplier contractual regimes excluding training on inputs and outputs. Necessary operational review is limited to providing the controller's service. No-training does not mean zero supplier security retention.

3. Subprocessors and international transfers

The controller generally authorises the subprocessors in Appendix 3. Equivalent protection duties are imposed on them and the processor remains responsible to the controller for their performance. Additions or replacements are notified at least 15 days in advance. The controller may reasonably object; if unresolved, it may terminate the affected service before the change without penalty. D-ID and HeyGen are not authorised as active suppliers by this appendix.

Transfers outside the EEA require Chapter V GDPR safeguards: an adequacy decision, with the US DPF only for the particular currently certified recipient, or standard contractual clauses and necessary supplementary measures. A European database region is not a promise of exclusively European processing. Relevant supplier agreements, recipients and transfer mechanisms must be verified before use; details are available on request.

4. Assistance, incidents and audit

The processor helps with data subject requests and Articles 32-36 duties including impact assessments and consultation. Requests received directly are forwarded without undue delay; the processor does not decide them independently without instructions or a legal duty.

Personal data breaches are notified without undue delay, contractually no later than 48 hours after awareness, with available information about scope, consequences, contact and measures. Missing information follows progressively. This upper limit does not justify delay or change the controller's statutory notification duties.

The processor provides the information needed to demonstrate compliance with Article 28 GDPR and permits a reasonable audit by the controller or an independent auditor appointed by it. A routine audit may be carried out no more than once every 12 months on written notice delivered at least 30 days in advance, in a manner that protects other

customers' data and system security; documentation may be provided before any on-site review. An extraordinary audit following a reasonable suspicion of a serious breach, an incident or a request from a supervisory authority is not restricted by this. Each party bears its own routine costs unless agreed otherwise; the controller's statutory rights are not affected.

Where the processor suffers damage causally connected with an unlawful instruction or a breach of the controller's obligations, in particular the lack of a legal basis for the processing or for contacting individuals, the controller shall compensate it to the extent the damage is attributable to the controller's breach and the law permits such compensation. Compensation includes reasonable costs of proceedings and legal representation, amounts paid to data subjects or third parties, and fines imposed by a final decision, if and to the extent mandatory law does not exclude their compensation. The processor shall document the existence, amount and causal link of the claim and take reasonable steps to limit the damage. The controller does not compensate the part of the damage attributable to the processor's own breach. This does not affect data subjects' rights, supervisory authorities' powers or the processor's own liability under the GDPR; the arrangement does not transfer public-law liability for a fine to another person.

5. Duration, end, liability and changes

Processing lasts only for the service and within Appendix 1 limits. At the end we return or delete data and copies as instructed unless law requires retention. Export is available before termination; production deletion is completed within 14 days. Backups remain isolated from ordinary use until expiry and deletions are reapplied upon restoration. The active backup cycle is supplied on request.

Separately retained accounting or contract evidence does not authorise retention of client conversations.

The processor's total liability to compensate the controller for damage under this DPA is limited to the amount of payments received from the controller for the AI Presenter service in the 12 months before the damaging event. The limit does not apply to damage caused intentionally or by gross negligence, to data subjects' rights under Article 82 GDPR, or to any other liability that cannot be limited under mandatory law, including the protection of natural rights of a person and the rights of a weaker party under section 2898 of the Czech Civil Code. Supervisory authorities' powers and statutory recourse claims are not restricted to the extent they cannot be limited by contract. This provision applies notwithstanding the precedence of the DPA over the terms and conditions.

Changes are notified at least 15 days in advance and changes requiring acceptance apply only after recorded acceptance. The [Czech version](#) prevails. [Version archive](#).

Appendix 1: AI Presenter processing

- Data subjects: client presentation visitors and the controller's prospects.
- Data: text/voice transcripts, topics and interests, voluntarily supplied name, email, phone and company, notice acknowledgement and separate consent records, technical/browser information and pseudonymised IP. Special-category data is not intended.
- Purpose: interactive presentation, answers, requested summary or quote and context handoff to the controller; later contact under a separate controller legal basis.
- Operations: transmission, storage, LLM processing, voice processing and TTS, display, evaluation, email, export and deletion.
- Duration: during the contract, at most 12 months from the session, or shorter on documented controller instruction. Current automatic operation removes transcripts and detailed events after 90 days, not contacts and all related records. The processor must delete remaining personal data separately under the instructions and contractual deadline; this does not represent automatic 12-month contact deletion as already deployed. Later contact capture does not restart the maximum session period. Section 5 applies at termination.
- Voice: current voice mode streams microphone audio through the server interface to Google Gemini for recognition, response and voice. This is not merely browser transcription. The application stores text transcripts, not an archive of microphone recordings. Google security retention follows its contractual regime. Typing is available without enabling a microphone.

Appendix 2: Technical and organisational measures

Transport uses HTTPS/WSS. Infrastructure storage/database encryption is provided by the platform, not custom field encryption. Supabase Auth manages passwords. AI keys and privileged database credentials are not in visitor code.

Presenter data is in a separate database schema with RLS, accessed through server functions checking service administrator or explicitly assigned operator permissions for each presentation. Personalised links and invitations use time-limited signed tokens; IP addresses are pseudonymised for limits. No absolute-security guarantee is made.

Session length/rate limits, input validation and anti-automation protection are used. Contract acceptance must be evidenced separately from voluntary visitor consent; an older acceptance of different terms is not acceptance of this DPA. Access, backup settings, retention jobs and restore procedures require operational verification; the actual backup plan must be evidenced in the active account. End-user operator MFA and a new automated consent ledger are not represented as deployed.

Appendix 3: Subprocessors

Supplier	Function	Location and limitations
Supabase	Database, authentication, files and server functions	Primary project database Frankfurt, eu-central-1; supplier access governed by its DPA
Vercel	app.salesrobots.cz hosting and technical operation	Global infrastructure; processing outside the EEA is possible; no EU-only promise
Google Gemini	LLM, live voice processing and TTS	Business regime without input/output training; possible temporary security logs and processing outside the EEA under Google terms
Google reCAPTCHA Enterprise	Protection against automated abuse when a presentation starts (risk assessment from browser and technical visitor data)	Processed by Google; processing outside the EEA is possible under Google terms
Resend / Plus Five Five, Inc.	Email summaries and notifications	Supplier DPA states primary US processing; EU sending region does not guarantee EU storage; SCC safeguards

Supplier documents: [Supabase](#), [Vercel](#), [Google Gemini](#), [Google Cloud \(reCAPTCHA Enterprise\)](#), [Resend](#). Public links do not prove acceptance in a particular account. Google's exact region and security retention depend on the service/configuration; this agreement promises neither zero retention nor EU-only processing.