

Privacy Policy

Last updated: 06.07.2026

1. Introduction and Data Controller

Welcome to the privacy policy of KLAI ("KLAI," "we," "us," "our"). This privacy policy explains what personal data we collect, how we use it, with whom we share it, and what rights you have in connection with this data when you use our web application and our AI assistant for room analysis and furnishing recommendations.

This privacy policy applies to all visitors of our website as well as to all users of the KLAI service, regardless of whether they use the service as registered users or anonymously (as a guest).

The controller responsible for data processing within the meaning of the General Data Protection Regulation (GDPR) is:

Klaudija Zubčić d.o.o. za dizajn interijera

Ribnjak 16
10000 Zagreb
Croatia

OIB (Personal Identification Number): 41501729818

MBS (Company Registration Number): 081372013

Commercial Court of Zagreb

Contact email: support@klai.design

("KLAI," "we," "us")

The external service providers listed below (OpenAI, Anthropic, AgentSight, [Bunny.net](#), Qdrant, Railway, Stripe, [SMTP provider]) act as processors or sub-processors. They process personal data on our behalf and in accordance with our instructions, based on corresponding data processing agreements and/or their respective terms of use.

Google and Apple, insofar as you use them for login, act as independent authentication providers in accordance with their own privacy policies. They are not sub-processors of KLAI, but rather independent controllers for the data they process in connection with OAuth login.

2. What Data We Collect

2.1 Account-Related Data

To use certain features (e.g., saving chat history, purchased recommendations, etc.), you can register and log in to a user account. The basic AI features are also available without registration as part of an anonymous guest session.

During registration/login, we collect the following data:

- First and last name
- Email address
- Password (stored exclusively in hashed form using bcrypt, never in plain text)
- If you log in via Google or Apple: your name, your email address, and (for Google) your profile picture, to the extent this information is provided by these providers in accordance with your privacy settings.

Login via Google and Apple takes place using the OAuth protocol. KLAI has no access to your Google or Apple password and does not store it.

If you forget your password, we will send a password reset link containing a time-limited token to the email address you provided.

Anonymous use (guest):

If you use KLAI without registering, you will be assigned a temporary, randomly generated guest ID (e.g., `guest_...`), which is stored in your browser's local storage. This identifier contains neither your name, email address, nor any other personal data, and is not linked to such data unless you register at a later time, thereby linking the existing guest chat to your newly created user account.

2.2 Data Related to the AI Assistant, Chats, and Photos

When using the AI assistant, the following data may be collected and processed:

- Questions and messages you send to the AI assistant
- Responses generated by the AI assistant
- Photos you upload (rooms, furniture, materials, or samples for comparison)
- Results of the AI room analysis (room type, dimensions, materials, colors, furniture overview, as well as your requirements — which elements should be kept or removed)
- Date and time of the interaction
- Conversation ID as well as — if you are logged in — your user account identifier
- Email address (if provided for delivery of a recommendation or as part of the Stripe payment process)
- Payment information processed via Stripe (KLAI does not store credit card or payment data; this is processed exclusively by Stripe)
- Language of the user interface/interaction

We do not require or expect users to provide personal data in order to use the basic AI analysis. An email address and payment information are only collected if you choose to purchase a recommendation or service.

2.3 Forms for Collecting Personal Data

Form	Data Collected	Purpose
Registration	First and last name, email address, password	Creating a user account
Login	Email address, password	Access to the user account
Forgot password	Email address	Sending a password reset link
Feedback	Free text, linked to the conversation ID and — if logged in — your user account	Improving the service

We do not collect your address or payment card data through our web forms. Payment data is processed exclusively directly by Stripe.

3. Cookies and Browser Storage (Local Storage)

3.1 Cookies

KLAI uses exclusively cookies that are technically necessary for the operation of the web application (authentication and security). We do not use cookies for marketing or analytics purposes.

Cookie Name	Purpose	Type
authjs.session-token / __Secure-authjs.session-token	Maintaining the logged-in user session	Necessary, HttpOnly
authjs.csrf-token / __Host-authjs.csrf-token	Protection against CSRF attacks during login	Necessary, HttpOnly
authjs.callback-url / __Secure-authjs.callback-url	Redirection after login via Google or Apple	Necessary, HttpOnly
authjs.pkce.code_verifier, authjs.state, authjs.nonce	Security parameters for OAuth login (Google/Apple)	Necessary, HttpOnly

NEXT_LOCALE	Stores the selected user interface language	Necessary (functional), contains no personal data
-------------	---	---

Since these are exclusively technically necessary cookies required for the operation of the service (login, security, and language settings), no prior consent via a cookie banner is required under the GDPR and ePrivacy regulations.

Since KLAI uses only technically necessary cookies, no prior consent via a cookie banner is required for their use.

3.2 Browser Local Storage and Session Storage

Key	Content	Purpose
guest_customer_id (Local Storage)	Randomly generated guest ID	Recognition of anonymous users across multiple sessions without registration
pending_conversation_id (Session Storage)	Conversation ID	Temporary linking of a guest chat to a user account after OAuth login (Google/Apple); deleted immediately after use

This data is stored locally in your browser. It does not contain any direct personal data (such as name or email address) and serves exclusively functional and technical purposes.

3.3 Web Analytics and Tracking

KLAI currently does not use any web analytics, user behavior, or error monitoring tools (e.g., Google Analytics, Plausible, Microsoft Clarity, Meta Pixel, Sentry, Hotjar, or PostHog).

4. Photos and AI Processing

KLAI uses artificial intelligence to analyze photos of rooms, furniture, and materials, and to create furnishing recommendations.

4.1 Processing Workflow

1. Via the chat or a form, you submit a request, a room description, and/or photos (of rooms, furniture, or materials/samples).

Photos uploaded through the user interface are transmitted directly to the AI backend

service for processing. There is no direct upload from the browser to CDN storage.

2. Before processing, photos are automatically checked (protection against misuse and prompt injection attacks) and compressed if necessary.
3. The AI assistant analyzes the content (text and/or image) and generates a response, a room analysis, or a product recommendation.
4. The data resulting from the interaction is stored for the purposes described in this privacy policy.

Our web application does not permanently store photos or conversation content locally in your browser.

4.2 Storage of Photos

- Photos are transmitted to external AI service providers (see table in Section 7) to generate analyses and recommendations.
- Photos are stored in [Bunny.net](#)'s CDN storage so that they can be displayed within the conversation and accessed again later as part of your recommendations.
- Photos remain linked to your user account solely for the purpose of displaying previous conversations and recommendations, and are permanently removed upon deletion of your user account.

4.3 Use of Data for Training AI Models

We do not use your photos or any other data you provide to train our own AI models.

Photos and other data are transmitted exclusively for the purpose of generating real-time responses and analyses to external AI service providers (OpenAI and Anthropic).

These providers process the data in accordance with their own terms of use and privacy policies, over which we have no direct influence or access.

Under the current terms of these providers, data transmitted via their APIs is by default not used to train their models. Please refer to the respective privacy policies of these providers for further information.

5. Purposes of Data Processing

We use the collected data for the following purposes:

- Providing and operating the AI assistant and the room analysis you requested
- Creating furnishing recommendations, product comparisons, and material matching

- Managing your user account and maintaining conversation context
- Identifying and resolving technical issues
- Analyzing and improving the quality of AI-generated responses and recommendations
- Processing payments and sending purchased recommendations via email
- Conducting security checks (protection against misuse and prompt injection attacks)

6. Legal Bases for Processing

The processing of your personal data is based on the following legal bases under the General Data Protection Regulation (GDPR):

- **Performance of a contract or pre-contractual measures (Art. 6(1)(b) GDPR)** – for managing your user account and providing the AI analyses and recommendations you requested.
- **Legitimate interest (Art. 6(1)(f) GDPR)** – to ensure the security, maintenance, and continuous improvement of our services.
- **Consent (Art. 6(1)(a) GDPR)** – when you voluntarily provide personal data (e.g., your email address for delivery of a recommendation) or log in via Google or Apple. In this case, consent is given to the respective provider in accordance with its privacy policy.

7. External Service Providers / Processors

To provide our services, we use the external service providers listed below. Each of these providers processes personal data on our behalf based on a data processing agreement and/or its respective terms of use.

Service Provider	Function	Location of Processing
OpenAI	AI language model (API), review of messages and images, generation of text embeddings, and fallback model for image analysis	USA
Anthropic (Claude)	AI language model (API), primary analysis of photos of rooms, products, and materials, generation of recommendations, and conversation management	USA
AgentSight	Storage and management of conversation content (messages, analysis results, and images) to provide the service, review of conversations, and improvement of service quality	Amsterdam, Netherlands (EU)
Bunny.net	CDN storage of photos uploaded by users	Frankfurt am Main, Germany (EU)

Qdrant	Vector database for searching the internal catalog of reference rooms (no personal or user-related data is stored)	Amsterdam, Netherlands (EU)
Railway	Hosting of the PostgreSQL database, AI agents, frontend, and Redis services	Amsterdam, Netherlands (EU)
Stripe	Payment processing	EU / USA (in accordance with Stripe's privacy policy)

In addition, Google and Apple, insofar as you log in via their services, act as independent authentication providers (OAuth) in accordance with their own privacy policies. They are not processors of KLAI, but rather independent controllers for the personal data processed as part of the login.

The list of service providers may occasionally change as the KLAI platform continues to develop. In such cases, we will always publish an updated version of this privacy policy.

We do not sell, rent, or trade your personal data.

Your data is disclosed exclusively to the above-mentioned service providers or in the following cases:

- when we are legally obligated to do so, by court order, or by a competent authority;
- in connection with a merger, acquisition, or transfer of our company, while ensuring an equivalent level of data protection; or
- when you have expressly consented to the disclosure.

8. International Data Transfers

Our hosting and storage infrastructure is located within the European Union (Netherlands – Railway).

If messages or photos are processed by our AI service providers (OpenAI and Anthropic), personal data may be transferred to the United States.

Such data transfers take place based on appropriate safeguards under the GDPR, in particular through the conclusion of Standard Contractual Clauses (SCCs) and/or through the respective providers' participation in the EU–US Data Privacy Framework, to the extent provided for under their privacy policies.

9. Retention Period

We store personal data only for as long as is necessary for the purposes described in this privacy policy.

In particular, the following retention periods apply:

- Conversation data and results of the AI analysis are stored until you delete your user account.
- Photos are generally stored until your user account is deleted and are then permanently removed from CDN storage and associated systems.
- Temporary technical data (e.g., image metadata in the Redis cache) is automatically deleted after seven (7) days.
- You may request the deletion of your personal data at any time before the expiration of the periods stated above (see Section 12 "Your Rights").

10. Data Security

We implement appropriate technical and organizational measures to protect your personal data.

These include, in particular:

- encryption of data transmission using HTTPS/TLS,
- restricting access to personal data to authorized personnel only,
- storing data within the European Union,
- and storing passwords exclusively in hashed form (bcrypt).

Although absolute protection of personal data cannot be technically guaranteed, we implement appropriate security measures to protect your data against unauthorized access, loss, misuse, or unlawful processing.

11. Reporting of Data Breaches

In the event of a personal data breach, we will notify the competent supervisory authorities and, where legally required, the affected users without undue delay, in accordance with the obligations under the GDPR.

12. Rights of Data Subjects

In connection with your personal data, you have the following rights:

- **Right to access** – You can request information about what personal data we process about you.
- **Right to rectification** – You can request the correction of inaccurate or incomplete data.

- **Right to erasure** – You can request the deletion of your personal data, subject to the retention periods stated in Section 9.
- **Right to restriction of processing**
- **Right to data portability**
- **Right to object to processing based on legitimate interests**
- **Right to withdraw consent at any time**, without affecting the lawfulness of processing carried out before the withdrawal
- **Right to lodge a complaint with a supervisory authority**

To exercise these rights, you may contact us at any time using the contact details provided in Section 15.

13. Protection of Minors

KLAI is not directed at persons under 18 years of age. We do not knowingly collect personal data from minors under this age limit.

If we discover that personal data of minors has been collected without appropriate parental or guardian consent, we will delete such data without delay.

14. Changes to This Privacy Policy

We reserve the right to update this privacy policy from time to time to reflect changes to our services, technologies, or legal requirements.

We will inform users of material changes through a notice on our website, together with the date of the last update at the beginning of this document.

We recommend that you review this page regularly.

15. Contact and Supervisory Authority

If you have questions about the processing of your personal data or wish to exercise your rights under Section 12, you can contact us at the following email address:

support@klai.design

Klaudija Zubčić d.o.o. za dizajn interijera
Ribnjak 16
10000 Zagreb
Croatia

OIB: 41501729818
MBS: 081372013
Commercial Court of Zagreb

Competent Data Protection Supervisory Authority:

Croatian Personal Data Protection Agency (AZOP)

Selska cesta 136
10000 Zagreb
Croatia

azop.hr

16. Applicable Law

This privacy policy and the data processing described herein are governed by the law of the Republic of Croatia and the law of the European Union, including the General Data Protection Regulation (GDPR).