

PRIVACY POLICY

Last updated on May 14, 2026.

The privacy policy of the **KLARA AI EUROPE, SOCIEDAD DE RESPONSABILIDAD LIMITADA** ("KLARA AI", "we", "our") contains information about how and why we may process your personal data (user data) when you use our services ("Services"), for example, when you:

- use our application - **Klara AI** ("App"), which contains a link to this Privacy Policy ("Services");
- interact with us in other ways, including any sales, marketing, etc.

"Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by an identifier such as a name, an identification number, location data, an online identifier, or by one or more factors that determine the physical, physiological, genetic, mental, economic, cultural or social essence of such a natural person.

"Processing" means any operation or series of operations with personal data or sets of personal data with or without the use of automated means, such as collection, registration, organization, structuring, storage, adaptation or modification, retrieval, review, use, disclosure by transmission, distribution or otherwise making available, arrangement or combination, restriction, erasure or destruction.

Other terms used in this Policy apply in the meanings given in General Data Protection Regulation (GDPR).

We process your personal data exclusively in the manner described in this Privacy Policy and in compliance with the requirements of legality and legitimacy. This Privacy Policy outlines our practices regarding the retention and protection of your personal data. Specifically, it details the measures we implement to securely retain your data and the safeguards in place to protect it from unauthorized access, disclosure, or misuse.

Question? Reading this Privacy Policy will help you understand your privacy rights and entitlements. If you do not agree with our policies and practices, please do not use our Services. If you still have questions or doubts, contact us at compliance@theklara.com.

SUMMARY OF KEY POINTS

Personal Data Controller

KLARA AI EUROPE, SOCIEDAD DE RESPONSABILIDAD LIMITADA, a legal entity incorporated under the laws of Spain, having its registered office at CL PALANGRE Num 13 39 3540 ALICANTE, ALICANTE.

Please refer to Section 3, titled "WHEN AND WHO DO WE SHARE YOUR PERSONAL DATA?", for detailed information regarding the third parties that may act as controllers of your personal data.

What personal data do we process? When you visit, use or link to our Services, we may process personal data based on your consent based on how you interact with KLARA AI, the Services and the choices you make, and the products and features you use.

Use a detailed list of personal data to which we may request access from you is provided in Section 1 “*WHAT PERSONAL DATA DO WE COLLECT? HOW DO WE GET ACCESS TO YOUR DATA?*”

How do we get access to your personal data? Access to your personal data may include filling in a box with a check mark when using our app, choosing technical settings for Services or behavior that clearly indicates the User's consent to the proposed processing of personal data. We adhere to the principle of transparency, which requires that any information and notices regarding the processing of personal data are accessible and understandable, using clear and simple wording so that the User is aware of the facts and limits of consent.

We collect data that you voluntarily provide to us when you express an interest in receiving information about us or our products and Services, when you participate in activities within the Services, or when you otherwise interact with us. Whenever possible, we request access to user data in context (via additional authentication) so that users understand why we need the data.

For what purpose and how do we process your personal data? We process your personal data to provide, improve and administer our Services, communicate with you, for security and fraud prevention, and to comply with the law. We can process your personal data if we believe it is necessary to determine usage trends, effectiveness of our advertising campaigns, and to evaluate and improve our Services, products, and marketing. We may also process your personal data with your consent for other lawful purposes.

How do we store your personal data? We store your personal data exclusively in compliance with the requirements for their safety, integrity and a special regime of access to them, which excludes the possibility of familiarization, distribution and access to personal data of Users directly or indirectly by third parties. We process personal data exclusively in a way that ensures an appropriate level of security and confidentiality of personal data, including to prevent unauthorized access or use of personal data, as well as equipment necessary for processing and against accidental loss, destruction or damage, using appropriate technical and organizational tools. You could read a more detailed description in Section 5 “*HOW DO WE STORE AND PROTECT YOUR DATA?*”.

Do we provide (transfer) access to your personal data to third parties? We may share personal data in specific situations and with specific third parties. A comprehensive list of such situations is defined in Section 3 “*WHEN AND WHO DO WE SHARE YOUR PERSONAL DATA?*”.

Do we process any sensitive information? We do not process confidential information.

Will we receive any information/data from third parties? We do not receive any information from third parties.

Want to know more about what KLARA AI does with any personal data we collect?

CONTENTS

1. WHAT PERSONAL DATA DO WE PROCESS? HOW DO WE GET ACCESS TO YOUR DATA?
2. FOR WHAT PURPOSE AND HOW DO WE PROCESS YOUR PERSONAL DATA?
3. WHEN AND WHO DO WE SHARE YOUR PERSONAL DATA?
4. HOW LONG DO WE KEEP YOUR PERSONAL DATA?
5. HOW DO WE STORE AND PROTECT YOUR DATA?
6. DO WE COLLECT PERSONAL DATA FROM MINORS?

7. WHAT ARE YOUR PRIVACY RIGHTS?
8. DO NOT TRACK CONTROLS
9. DO CALIFORNIANS HAVE SPECIAL PRIVACY RIGHTS?
10. DO WE UPDATE THIS POLICY?
11. HOW CAN YOU CONTACT US ABOUT THIS POLICY?

1. WHAT PERSONAL DATA DO WE PROCESS? HOW DO WE GET ACCESS TO YOUR DATA?

Personal data that you disclose to us.

In short: we collect personal data that you provide to us.

We collect data that you voluntarily provide to us when you express interest in receiving information about us or our products and Services, when you participate in activities within the Services, or otherwise when you interact with us.

Personal data provided by you. The personal data we process depends on the context of your interaction with us and the Services, the choices you make, and the products and features you use. Personal data that we process may include the following:

- pictures
- photos

Personal data that we process:

- User's name, e-mail address and contact phone number of the User.
- Profile data and other materials you post in the App. This may include your name, username, date of birth, email address and phone number. You may also provide us additional data on your Profile. This may include, but is not limited to: your gender and age, other personal characteristics and demographic data, any ideas, comments, testimonials you share and post, as well as images, photographs and videos. By providing this information you agree and understand that this data may be publicly available (unless otherwise explicitly stated in a particular case). Please do not provide personal data to your profile that you would not want to be publicly available.

We only request access to the minimum, technically possible amount of data that is necessary for us to implement the existing functions or services of our application. Whenever possible, we request access to user data in context (via additional authentication) so that users understand why we need the data.

Confidential information. We do not process confidential information.

Program data. If you use our applications, we may also process the following information if you choose to give us access or permission:

- *Mobile device access.* We may request access or permission to certain features from your mobile device, including your mobile device's camera and other features. If you want to change our access or permissions, you can do so in your device settings.

- *Push notifications.* We may ask to send you push notifications regarding your account or certain app features. If you want to opt out of receiving these types of messages, you can turn them off in your device settings.

This information is primarily necessary for the security and operation of our applications, for troubleshooting, and for internal analytics and reporting.

All personal data you provide to us must be true, complete and accurate, and you must notify us of any changes to such information/data.

HOW DO WE GET ACCESS TO YOUR DATA?

Access to your personal data may include filling in a box with a check mark when visiting our app, choosing technical settings for services or behavior that clearly indicates the User's consent to the proposed processing of personal data. We collect data that you voluntarily provide to us when you express an interest in receiving information about us or our products and Services, when you participate in activities within the Services, or when you otherwise interact with us. Whenever possible, we request access to user data in context (via additional authentication) so that users understand why we need the data.

2. FOR WHAT PURPOSE AND HOW DO WE PROCESS YOUR PERSONAL DATA?

In short: We use your personal data to provide, improve and administer our Services, communicate with you, for security and fraud prevention, and to comply with the law. We may also process your personal data with your consent for other purposes.

We process your personal data for various reasons, depending on how you interact with our Services, including:

- **to provide services to you.** This includes enabling you to use the Services in a seamless manner and preventing or addressing App's errors or technical issues.
- **to evaluate and improve our Services, products, and marketing.** We may *process* your personal data if we believe it is necessary to determine usage trends, the effectiveness of our advertising campaigns, and to evaluate and improve our Services, products, and marketing. This enables us to gain a deeper understanding of our business, analyze our operations, and maintain, improve, innovate, plan, design, and develop the App as well as our new products. We conduct surveys, research, and test features under development. The data we collect is analyzed to evaluate the App's performance, and we conduct audits and troubleshooting to enhance the App's content and layout. Consequently, decisions regarding improvements to the App are often based on the results of this processing. For example, if we determine that a particular section of the App is underutilized, we may prioritize enhancements to that section.
- **to enforce our Terms of Service and to prevent, detect, investigate, and resolve disputes, as well as to address malicious activities, fraud, cybercrime, or to take legally required actions, including verifying your identity and preventing the creation of fraudulent accounts.** We process personal data to enforce our contractual obligations and agreements, as well as to detect, prevent, and mitigate fraudulent activities. In connection with this processing, we may share your personal information with relevant third parties, including law enforcement agencies, particularly in the event of a dispute arising from a violation of the Terms.

- **to comply with legal obligations.** We may process, use, or share your data when the law requires it, in particular, if a law enforcement agency requests your data by available legal means.

If we need to further process personal data for a purpose other than the one for which the personal data was obtained, we will provide you with information about such other purposes and any relevant details specified in the General Data Protection Regulation data (GDPR).

Do we update your personal data?

We take all reasonable steps to update your data to ensure that inaccurate personal data, having regard to the purposes for which it was processed, is deleted or corrected without delay. You have the right to contact us to correct your personal data and the right to fill in incomplete personal data, including by submitting an additional statement.

What are the grounds for restricting personal data?

You have the right to contact us with a statement regarding the restriction of processing of your personal data in the event of the following circumstances:

- the accuracy of the personal data is contested by you, within a period of time that gives us the opportunity to check the accuracy of the personal data;
- the processing is illegal and you object to erasure of personal data and instead send a request to restrict their use;
- we no longer need your personal data for processing purposes, but you require them to form, exercise or defend legal claims;
- you object to processing pending a review of whether our legitimate grounds override your legitimate interests.

We keep records of processing of personal data, which include, among other things, information about: description of categories of data subjects and categories of personal data; categories of recipients to whom personal data has been or will be disclosed, including recipients in third countries or international organizations; if possible, — time limits are provided for erasing different categories of data; if possible, — a general description of technical and organizational security measures; other mandatory information according to the General Data Protection Regulation (GDPR).

3. WHEN AND WHO DO WE SHARE YOUR PERSONAL DATA?

In short: We may share personal data in the specific situations described in this section and/or with the following third parties.

We may need to provide your personal data in the following situations:

- **Organizational processes.** We may share or transfer your information (data) in connection with or during negotiations for any merger, sale of company assets, financing or acquisition of all or part of our organizational activities by another company. We transfer your personal data to individuals and legal entities that comply with the terms of the General Data Protection Regulation (GDPR).

3.1. Which third parties may receive your personal data with the use of our Services?

Banking Institutions

When you use specific Services with the use of our App, including but not limited to Loan Acquisition Assistance and Transaction and Account Management Services, your personal data may be processed and transferred to banking institutions that facilitate these services. Full information about the banking institution to which your personal data will be transferred will be indicated in our application at the time of filling in such data and ticking the box indicating your consent to the transfer.

Transfer of Personal Data: The personal data you provide through our application in connection with these Services will be securely transferred to the relevant banking institutions. This transfer is necessary for the performance of the contract between you and the banking institution.

Responsibility for Data Protection: Upon the transfer of your personal data to the banking institutions, these entities become the data controllers with respect to the personal data they receive. As data controllers, they are responsible for the processing and protection of your personal data in accordance with their own internal policies and the requirements of the GDPR.

Banking Institutions' Compliance: We ensure that all banking institutions we collaborate with are bound by contractual agreements to process your personal data in compliance with GDPR standards, including the implementation of appropriate technical and organizational measures to safeguard your data.

Your Rights: You retain all rights afforded to you under the GDPR, including the right to access, rectify, or request the deletion of your personal data. If you have any concerns about how your personal data is processed by the banking institutions, you should contact them directly as the data controller.

3.2. To whom we could transfer your personal data?

KYC providers

When you use specific Services provided by us, your personal data may be processed and transferred to third-party KYC (Know Your Customer) providers that assist in verifying your identity and ensuring compliance with legal and regulatory requirements.

Transfer of Personal Data: In connection with these Services, the personal data you provide through our application will be securely transferred to the KYC providers with whom we have a contractual relationship.

Responsibility for Data Protection: Upon the transfer of your personal data to the KYC providers, these entities become the data controllers with respect to the personal data they receive. As data controllers, they are responsible for the processing and protection of your personal data in accordance with their internal policies and the GDPR.

KYC Providers' Compliance: We have entered into contracts with all KYC providers we work with, requiring them to process your personal data in strict compliance with GDPR standards, including the implementation of appropriate technical and organizational measures to ensure the security and confidentiality of your data.

Your Rights: You retain all rights under the GDPR, including the right to access, rectify, or request the deletion of your personal data. If you have concerns regarding the processing of your personal data by the KYC providers, you should contact them directly as the data controller.

International data transfers

Some of our service providers and partners are located outside the European Economic Area, primarily in the United States. For all such transfers, we rely on appropriate safeguards under Article 46 GDPR, including:

- **Adequacy decisions** of the European Commission (e.g., EU-U.S. Data Privacy Framework for certified U.S. recipients)
- **Standard Contractual Clauses** approved by the European Commission
- Additional technical and organizational measures where required

A copy of the safeguards applied to a specific transfer is available upon request to Compliance@theklara.com.

3.3 AI Service Providers

When you use the Klara AI chat feature, the text of your messages is transmitted to third-party AI service providers acting as data processors on our behalf:

- **OpenAI, L.L.C.** (United States) — openai.com/privacy
- **Google LLC** (United States) — for Gemma model processing — policies.google.com/privacy

Klara does not attach personal identifiers to these requests. AI providers process messages strictly to generate responses and do not use this data to train their models. Users are informed and provide explicit in-app consent prior to first use of the AI chat feature. Consent can be withdrawn at any time in Profile → Settings → Privacy & Legal → AI Chat.

3.4 Marketing, Attribution and Advertising Partners *(по имени, обязательно)*

We work with third-party marketing partners who act as independent or joint data controllers for advertising attribution, campaign measurement, and targeting purposes. Data shared may include device identifiers (IDFA, IDFV), advertising IDs, install events, in-app conversion events, and aggregated usage metrics.

Current partners:

- **Meta Platforms, Inc.** (Facebook, Instagram) — facebook.com/privacy
- **Google LLC** (Google Ads, Google Analytics, Google Play) — policies.google.com/privacy
- **AppsFlyer Ltd.** — appsflyer.com/legal/privacy-policy
- **Adkomo** — adkomo.com/privacy
- **Virtuads** — virtuads.com/privacy
- **Apple Inc.** (Apple Search Ads, App Store analytics) — apple.com/legal/privacy

We may also engage additional advertising partners in the future, which may include but are not limited to: Reddit Ads, TikTok Ads, LinkedIn, YouTube Ads, influencer and affiliate marketing platforms. The current list of active marketing partners is available upon request to compliance@theklara.com.

Data is shared with these partners only after the user grants permission via the App Tracking Transparency (ATT) prompt on iOS. Users can revoke this permission at any time in their device settings (Settings → Privacy & Security → Tracking).

3.5 Analytics and Technical Service Providers *(категории, имена опциональны)*

We engage third-party service providers that act as data processors strictly on our behalf to support the operation of our Services. These providers do not use the data for their own purposes. Categories include:

- **Customer data platform** — for routing event data between our systems and partners (currently: Segment, Inc.)
- **Product analytics providers** — for understanding feature usage and improving the Services (currently: PostHog)
- **Crash reporting and monitoring providers** — for diagnosing technical issues
- **Push notification service providers** — for delivering in-app notifications
- **Fraud prevention providers** — for detecting and preventing fraudulent activity
- **CRM and email communication providers** — for transactional and marketing communications

A current and complete list of processors is available upon request to compliance@theklara.com. All processors are bound by data processing agreements under Article 28 GDPR.

4. HOW LONG DO WE KEEP YOUR PERSONAL DATA?

In short: We take all necessary measures to ensure that the period during which personal data is stored is reduced to an absolute minimum. The criteria for determining the period of storage of the User's personal data are the achievement of the goal(s) defined in Section 2 "FOR WHAT PURPOSE AND HOW DO WE PROCESS YOUR PERSONAL DATA?".

Data retention

The retention period is determined based on the following criteria:

- the duration of your use of our Services;
- the necessity of the data for the purposes outlined at the time of collection;
- legal obligations to which we are subject (e.g., tax, accounting, or regulatory requirements);
- our legitimate business interests, such as maintaining security, preventing fraud, and improving our services.

We will retain personal data for as long as necessary to fulfill the purposes outlined in this Policy, unless a longer retention period is required or permitted by applicable law.

When you delete your account, we will retain your personal data for a period of 1 month from the date of deletion. This retention period allows us to comply with our legal obligations, resolve disputes, and enforce our agreements. After this period, your data will be permanently deleted or anonymized unless we are required to retain it longer by law. During this time, your data will be securely stored and will not be processed for any other purpose.

Please be aware that we are subject to various legal obligations to retain the data you provide, including to assist in the identification and prevention of fraud, and to comply with anti-money laundering regulations and other applicable laws and regulations governing our operations and those of our financial service providers. Therefore, even if you choose to deactivate or delete your Profile, we may retain certain personal data to fulfill these legal and regulatory obligations.

Data Disposal

When your personal data is no longer needed for the purposes for which it was collected, or when you request its deletion, we ensure that it is securely disposed of in compliance with GDPR requirements. Our data disposal practices include:

Secure Deletion: Personal data is deleted using methods that ensure it cannot be reconstructed or recovered. This may include the use of secure deletion tools or processes that permanently erase data from our systems.

Anonymization: In cases where the data cannot be fully deleted, or where deletion is not feasible, we may anonymize the data so that it no longer identifies you or can be linked back to you.

Third-Party Disposals: Where third-party service providers process personal data on our behalf, we ensure that they are contractually obligated to follow similar secure disposal practices, in compliance with the GDPR.

Your Rights

In short: If you wish to exercise your right to erasure, please contact us at compliance@theklara.com. We will respond to your request in accordance with GDPR timelines and requirements.

You have the right to delete your personal data and stop processing it ("right to be forgotten") if:

- the personal data is no longer necessary for the purposes for which we collect it or otherwise process it,
- you had withdrawn your consent or objected against the processing of your personal data, and if there is no other lawful basis for the processing, or if the processing of your personal data otherwise does not comply with the General Data Protection Regulation (GDPR).

In the event of receiving a request for erasure of personal data and in the event of providing your personal data to third parties (in accordance with Section 3), we take appropriate measures, including technical measures, to inform such third parties that process personal data that you have requested the erasure of any references to, copies of, or reproductions of such personal data.

We will only retain your personal data for as long as is necessary for the purposes set out in this Privacy Policy, unless a longer retention period is required or permitted by law (for example, tax, accounting or other legal requirements).

We may be required to erase your personal data to comply with a statutory obligation set out in the legislation that applies to us.

Unless we have an ongoing legitimate business need for the processing of your personal data, we will delete or anonymize such information (data).

5. HOW DO WE STORE AND PROTECT YOUR DATA?

We store your personal data exclusively in compliance with the requirements for their safety, integrity and a special regime of access to them, which excludes the possibility of familiarization, distribution and access to personal data of Users directly or indirectly by third parties.

We are committed to ensuring the security and confidentiality of your personal data. To protect your data, we implement a variety of technical and organizational measures designed to safeguard against unauthorized access, alteration, disclosure, or destruction. Our data protection practices are in strict compliance with the General Data Protection Regulation (GDPR) and are regularly reviewed and updated to maintain the highest security standards.

Encryption and Secure Storage: All personal data processed through our mobile application is encrypted both in transit and at rest using industry-standard encryption protocols. This ensures that your data is protected from unauthorized access during transmission and while stored on our servers.

Access Control: Access to your personal data is restricted to authorized personnel only. We employ strict access control measures, including multi-factor authentication, to ensure that only individuals with a legitimate need to access your data can do so.

Regular Security Audits and Penetration Testing: We conduct regular security audits and penetration testing to identify and address potential vulnerabilities in our systems. These assessments are performed by qualified security professionals to ensure that our security measures are effective and up-to-date.

Data Minimization and Anonymization: We adhere to the principle of data minimization, collecting and processing only the personal data necessary for the specified purposes. Where possible, personal data is anonymized to further protect your privacy.

Incident Response and Breach Notification: In the event of a data breach, we have a comprehensive incident response plan in place. We will notify the relevant supervisory authorities and affected individuals without undue delay, and within the timeframes required by the GDPR, should a breach pose a high risk to your rights and freedoms.

Data Retention and Disposal: We retain your personal data only for as long as necessary to fulfill the purposes for which it was collected, in accordance with our Data Retention Policy. When your data is no longer needed, it is securely deleted or anonymized.

Third-Party Service Providers: Where we engage third-party service providers to process personal data on our behalf, we ensure that they are bound by contractual obligations to implement appropriate technical and organizational measures to protect your data in compliance with the GDPR.

Your Rights and Our Responsibilities: We respect your rights under the GDPR, including your rights to access, rectify, erase, and restrict the processing of your personal data. Our responsibilities include ensuring that your data is processed lawfully, fairly, and transparently, and that your privacy is protected at all times.

For the purposes of this Policy and other requirements, this section is considered the Data Protection Policy and Data Retention Policy.

6. DO WE COLLECT PERSONAL DATA FROM MINORS?

In short: We do not knowingly collect or sell personal data from children under the age of 18.

We do not knowingly collect, process or share personal data from children under the age of 18. By using the Services, you represent that you are at least 18 years of age, or that you are the parent or

guardian of such a minor, and consent to the use of the Services by such minors. If we become aware that personal data has been collected from users under the age of 18, we will deactivate the account and take steps to immediately delete such data from our records. If you become aware of any information we may have collected from children under the age of 18, please contact us at compliance@theklara.com.

The right to delete his personal data is preserved, including when the User gave his consent as a child and was not fully aware of the risks associated with processing, and later wanted to delete such personal data. The user has the right to request the deletion of data, despite the fact that he is no longer a child.

7. WHAT ARE YOUR PRIVACY RIGHTS?

In short: You can review, change or terminate your account at any time.

- 1) **the right to receive information about your personal data** processed by us, the purposes of their processing, if possible, the period during which personal data is processed (if this is not possible, the criteria for determining such a period), the logic that conditions any automated processing of personal data, and receipt of confirmation and notification of those personal data that concern you and are subject to processing, the consequences of such processing, categories of relevant personal data.
- 2) **the right to receive a copy of personal data** that is in the process of processing. We will provide you with information in a concise, transparent, comprehensible and easily accessible form, using clear and simple wording, without unreasonable delay and in any case within one month from the date of receipt of the request.
- 3) **the right to withdraw your consent to the processing of your personal data** at any time. Withdrawal of consent does not affect the lawfulness of processing that was based on consent before its withdrawal.
- 4) **the right to limit the processing of your personal data or to object to processing, as well as the right to data portability.** You have the right to receive your personal data in a structured, generally accepted, machine-readable format and the right to transfer such data to another controller.
- 5) **the right to send a request for correction or erasure of your personal data;**
- 6) **the "right to be forgotten"** if there is no longer a need for personal data for the purposes for which they were collected or otherwise processed; if the retention of such data violates the General Data Protection Regulation (GDPR or Union or Member State legislation that applies to you. You have the right to withdraw your consent on which the processing is based.
- 7) **the right to file a complaint with a supervisory authority.**
- 8) **the right to know what personal information is being collected and to correct inaccurate information (if any).** You may review, edit, or change your personal data through your account settings or by emailing us at the email address compliance@theklara.com.
- 9) **the right to delete your personal data.** You can request the erasure of your personal data by emailing us at the email address compliance@theklara.com. In some cases, we may be legally required to keep some of the data for a certain time; in which case we will fulfill your request after we have complied with our obligations.

Depending on where you are geographically located, the relevant laws of your location may give you certain rights with respect to your personal data.

We take all reasonable steps to ensure that inaccurate personal data is corrected or deleted. In accordance with the applicable laws of your country, you may have the right to request access to the personal data we collect about you, to change this information or to delete it under certain

circumstances. To request a review, update or deletion of your personal data, please contact us at compliance@theklara.com.

How do I exercise my rights?

The easiest way to exercise your rights is to contact us: compliance@theklara.com. We will consider and apply the necessary measures to any request in accordance with the current legislation on the protection of personal data.

You may submit requests through an authorized agent, in which case we will need to verify the agent's identity, your identity, and their authority to act on your behalf before we can process the request. Depending on the applicable legislation, you may also be entitled to other/additional rights in relation to your personal data.

If you are located in the EEA or the UK and believe that we are unlawfully processing your personal data, you also have the right to lodge a complaint with your local data protection supervisory authority. Their contact details can be found here: https://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm.

If you are located in Switzerland, the contact details of the data protection authorities are available here: <https://www.edoeb.admin.ch/edoeb/en/home.html>.

If you are a resident of a U.S. state that has enacted applicable consumer data privacy laws, which include, but might not be limited to: California, Colorado, Connecticut, Utah and Virginia, you may be entitled to specific rights, including those regarding access to your personal information. However, please note that such laws usually have a certain applicability threshold, and, thus, may not be fully applicable to App. For more information, please contact us at the email address compliance@theklara.com.

Withdrawal of your consent: if we rely on your consent to process your personal data, which may be express and/or implied consent depending on applicable law, you have the right to withdraw your consent at any time. You may withdraw your consent at any time by contacting us at the contact details provided under HOW CAN YOU CONTACT US ABOUT THIS POLICY? lower.

Please note, however, that this will not affect the lawfulness of the processing prior to withdrawal, nor, if permitted by applicable law, will it affect the processing of your personal data that is carried out on the basis of lawful processing.

If you have any questions or comments about your privacy rights, you can email us at compliance@theklara.com.

8. Tracking Technologies and ATT

Tracking on iOS — App Tracking Transparency

On iOS, before any tracking activity for attribution or advertising purposes occurs, Klara displays Apple's App Tracking Transparency (ATT) prompt requesting your explicit permission. If you decline:

- We do not share your device identifiers with advertising partners
- You will not receive personalized advertising attribution
- Core app functionality is not affected

If you accept, your IDFA may be used for install attribution and shared with our marketing partners as listed in Section 3.4. You can revoke this permission at any time in Settings → Privacy & Security → Tracking on your device

9. DO CALIFORNIA RESIDENTS HAVE SPECIAL PRIVACY RIGHTS?

In short: Yes, if you live in California, you have certain rights regarding access to your personal information.

California Civil Code Section 1798.83, also known as the "Shine The Light" law, allows our users who are residents of California to request and receive from us once a year, free of charge, information about categories of personal information/data (if any) disclosed to third parties for direct marketing purposes, and the names and addresses of all third parties with whom we have shared personal data during the previous calendar year. If you reside in California and wish to make such a request, please send us a written request using the contact information below.

If you are under the age of 18, live in California and have a registered account on our Services, you have the right to request the removal of unwanted data that you publicly post on the Services. To request deletion of such data, please contact us using the contact information below and include the email address associated with your account and a statement that you are a California resident. We will take care not to display data publicly on the Services, but please be aware that data may not be completely removed from all of our systems (eg backups, etc.).

10. DO WE UPDATE THIS POLICY?

In short: Yes, we will update this Policy as necessary to comply with legal requirements.

We may update this Policy from time to time. The updated version will be listed as updated with a "Revised" note, and the updated version will be effective as soon as it becomes available. If we make material changes to this Privacy Policy, we may notify you by posting a notice of such changes in a prominent place or by sending you a notice directly. We encourage you to review this Policy frequently to stay informed of how we are protecting your information.

11. HOW CAN YOU CONTACT US ABOUT THIS POLICY?

If you have any questions or comments about this Policy, you can email us at compliance@theklara.com.

KLARA AI EUROPE, SOCIEDAD DE RESPONSABILIDAD LIMITADA, a legal entity incorporated under the laws of Spain, having its registered office at CL PALANGRE Num 13 39 3540 ALICANTE, ALICANTE.