Privacy Policy

Last updated: September 3, 2025

This Privacy Notice for **IntoClimb** (“we,” “us,” or “our”) describes how and why we access, collect, store, use, and/or share (“process”) your personal information when you use our services (“Services”), including when you:

- Visit our website at **intoclimb.com** or any other website of ours that links to this Privacy Notice
- Download and use our mobile application (**IntoClimb**), or any other application of ours that links to this Privacy Notice
- Use our Services, including interacting with us through sales, marketing, or events

---

About IntoClimb

IntoClimb is a modern app designed for indoor climbing gyms and their communities. Key features include:

- **Map**: An interactive floorplan of the gym, with routes created and managed by the gym
- **Routes**: Bouldering and lead routes with personalized grading systems, community grading, ratings, and labels
- **Feed**: A live feed from the gym to share updates, news, and offers with instant user notifications
- **Competition**: Tools for creating and managing competitions with features like grading-based scoring, attempt deductions, flash bonuses, and a live leaderboard
- **Profile**: Users can track progress, view rankings, and manage personal climbing data
- **About**: A customizable gym page with photos, embedded content, and auto-updated opening times

- **Admin Tools**: Statistics, role management, and tools for collaborative gym administration

---

Questions or Concerns?

Reading this Privacy Notice will help you understand your rights and our responsibilities. If you do not agree with our practices, please do not use our Services.
If you have any questions or concerns, contact us at **hello@intoclimb.com**.

Summary of Key Points

This summary outlines the main aspects of our privacy practices. For full details, please refer to the complete Privacy Notice.

What personal information do we process?

We may process personal information based on how you interact with our Services, the choices you make, and the features you use.

Do we process any sensitive personal information?

We do not process any data that is classified as “special” or “sensitive” under relevant laws (e.g., racial or ethnic origin, religious beliefs, sexual orientation).

Do we collect information from third parties?

No. We do not collect personal information from third-party sources.

How do we process your information?

We process personal data to provide and improve our Services, communicate with users, ensure security, prevent fraud, and comply with legal obligations. Processing is always based on a valid legal basis.

In what situations and with which parties do we share personal information?

We may share data in specific, limited contexts with designated third parties. These are outlined in the full Privacy Notice.

How do we keep your information safe?

We use appropriate technical and organizational measures to protect your data. However, no digital system can be guaranteed to be 100% secure.

What are your rights?

Depending on your geographic location, applicable privacy laws may grant you rights related to access, correction, deletion, objection, and data portability.

How do you exercise your rights?

You can exercise your rights by visiting **intoclimb.com** or contacting us directly. We will respond according to applicable data protection laws.

Want to learn more?

Please refer to the full Privacy Notice for detailed information about how we collect, use, and protect your personal information.

What Information Do We Collect?

Personal Information You Disclose to Us

In Short: We collect personal information that you provide to us.

We collect personal information that you voluntarily provide when you register for our Services, express interest in learning more about our products or services, participate in activities through the Services, or otherwise contact us.

Personal Information Provided by You

The types of personal information we collect depend on your interactions with us and the features you use. This may include:

- Name
- Email address

- Password (Stored safely using Google Authentication)

Sensitive Information

We do **not** process sensitive personal information (such as health data, biometric data, or information about racial or ethnic origin, religious beliefs, or sexual orientation).

Social Media Login Data

If you choose to register or log in to our Services using a social media account (e.g., Google, Apple), we may collect profile information from the relevant provider. More information is provided under the section titled **"How Do We Handle Your Social Logins?"**.

Application Data

When using our mobile application(s), we may collect the following information if you grant us access:

- **Mobile Device Access:** Access to certain features of your device (e.g., camera, storage). You can manage these permissions in your device settings.

- **Mobile Device Data:** We automatically collect data including your device ID, model, manufacturer, operating system and version, system settings, browser type, IP address, mobile carrier, and application usage data.

- **Push Notifications:** With your permission, we may send push notifications regarding your account or certain features. You can disable these in your device settings.

This data helps us ensure application security, troubleshoot technical issues, and perform internal analytics and reporting.

All personal information provided must be accurate, complete, and up-to-date. You are responsible for notifying us of any changes.

Information Automatically Collected

In Short: Some information—such as your IP address and browser/device characteristics—is automatically collected when you use our Services.

We collect certain technical data automatically when you access, use, or navigate our Services. While this information does not directly identify you, it may include:

- IP address
- Device and browser type and settings
- Operating system and language preferences
- Referring URLs
- Geographic location (such as country or city)
- Usage details (e.g., pages visited, actions taken, time spent)

This information is used for service optimization, internal analytics, and to ensure the security and reliability of our Services.

Examples of Automatically Collected Data

- **Log and Usage Data:** Server logs may include IP addresses, browser types, operating systems, device information, time/date stamps, pages visited, search queries, and diagnostic data (e.g., crash reports).

- **Device Data:** Device-specific information, such as model, system configuration, browser settings, and connection type.

Google API Usage

Our use of data obtained through Google APIs complies with the Google API Services User Data Policy, including its **Limited Use** requirements.

---

2. How Do We Process Your Information?

In Short: We process your information to provide and improve our Services, communicate with you, ensure security, and comply with legal obligations.

We may process your personal data for the following purposes:

- **Account Creation and Management:** To allow you to register, authenticate, and manage your account.

- **Security and Fraud Prevention:** To detect and prevent fraud or misuse of our Services.

- **Compliance with Legal Obligations:** To fulfill our legal and regulatory responsibilities.

- **Vital Interests:** To protect an individual's life or safety where necessary.

We will only process your information for other purposes with your explicit prior consent.

3. What Legal Bases Do We Rely On to Process Your Information?

In Short: We only process your personal information when we have a valid legal basis to do so under applicable law, including with your consent, to comply with legal obligations, to provide services, to fulfill contracts, to protect your rights, or to pursue legitimate business interests.

Under the General Data Protection Regulation (GDPR) and the UK GDPR, we rely on the following legal bases:

Consent

We may process your personal information if you have given us explicit permission to do so for a specific purpose. You may withdraw your consent at any time. For more information, see **“Your Privacy Rights”**.

Legal Obligations

We may process your information to comply with applicable legal obligations, such as cooperating with law enforcement, regulatory requirements, legal proceedings, or defending our legal rights.

Vital Interests

We may process your information when it is necessary to protect your vital interests or those of another person, such as in emergency situations involving threats to safety.

Other Legal Grounds

We may process your personal information without your consent under certain circumstances permitted by applicable law, including:

- If collection is clearly in the individual’s interest and consent cannot be obtained in a timely manner.
- For the purpose of investigating fraud or suspected unlawful activity.
- In connection with a business transaction, provided legal requirements are met.
- If required in a witness statement for the processing of an insurance claim.

- To identify or contact an injured, ill, or deceased individual’s next of kin.
- Where there are reasonable grounds to suspect financial abuse.
- If obtaining consent would compromise the accuracy or availability of the information needed for legal investigations.
- When disclosure is required by a subpoena, warrant, or court order.
- If information was created in the course of an individual's employment or profession and is used in a manner consistent with that purpose.
- When used solely for journalistic, artistic, or literary purposes.
- If the information is publicly available and as defined by regulation.
- For de-identified data used in approved research or statistical studies, subject to confidentiality and ethics requirements.

---

4. When and With Whom Do We Share Your Personal Information?

In Short: We may share your personal information with third parties under specific circumstances and with appropriate safeguards in place.

Third-Party Service Providers

We may share your data with vendors, consultants, contractors, and other third-party service providers who require access to the information to carry out work on our behalf. These parties are contractually obligated to:

- Use your personal information only as instructed by us;
- Maintain the confidentiality and security of the data;
- Refrain from sharing your data with other parties;
- Adhere to data protection standards consistent with applicable frameworks (e.g., the EU-U.S. and Swiss-U.S. Data Privacy Framework Principles).

Categories of third parties may include:

- User account registration and authentication providers
- Cloud computing services
- Data storage providers
- Data analytics services

Other Situations

- **Business Transfers:** We may share or transfer your information in connection with mergers, acquisitions, financing, or asset sales.

- **Business Partners:** We may share your information with business partners to offer certain products, services, or promotions.

---

5. Do We Use Cookies and Other Tracking Technologies?

In Short: Yes, we may use cookies and similar tracking technologies to enhance your experience and collect information about your usage of the Services.

We use cookies, web beacons, pixels, and similar technologies to:

- Maintain security
- Prevent bugs and crashes
- Store preferences
- Support essential functionality

Third-party service providers may also use these technologies for analytics and advertising purposes, including:

- Managing and displaying advertisements
- Customizing content based on your interests
- Sending reminders (e.g., abandoned cart emails)

Third-Party Tracking

Third parties may collect data across our Services and other websites to deliver advertising tailored to your interests. Where applicable, such activities may constitute a "sale" or "sharing" under certain U.S. state laws. You may opt out of such tracking by following instructions in the section **"Do United States Residents Have Specific Privacy Rights?"**.

For detailed information, including how to manage cookie preferences, please refer to our **Cookie Notice**.

Google Analytics

We use Google Analytics to understand and analyze usage trends. To opt out of Google Analytics tracking across our Services, visit: https://tools.google.com/dlpage/gaoptout
For more details on Google's data practices, see their Privacy & Terms page.

6. Do We Offer Artificial Intelligence–Based Products?

In Short: Yes, we offer features and tools powered by artificial intelligence (AI), machine learning, and similar technologies to enhance your experience.

As part of our Services, we provide products, features, and tools powered by artificial intelligence and machine learning (collectively, "AI Products"). These tools are designed to deliver innovative solutions and improve how you interact with our Services. This Privacy Notice governs your use of AI Products within our platform.

Use of AI Technologies

Our AI Products are provided in partnership with third-party service providers ("AI Service Providers"), including Google Cloud AI. To enable functionality, your inputs, outputs, and any personal information processed through the AI Products may be shared with these providers. Such processing is conducted in accordance with the legal bases outlined in the section **"What Legal Bases Do We Rely On to Process Your Information?"**.

Use of AI Products must comply with applicable terms and policies of the AI Service Providers.

Our AI Product Capabilities

Our AI Products currently support the following functionality:

- Image generation
- Natural language processing

How We Process Your Data Using AI

All personal information processed through our AI Products is handled in accordance with this Privacy Notice and the contractual safeguards in place with our service providers. These measures help ensure the privacy, confidentiality, and security of your data throughout its use.

---

7. How Do We Handle Your Social Logins?

In Short: If you choose to register or log in using a social media account, we may receive certain profile information from the social media provider.

Our Services allow you to register or sign in using credentials from third-party social platforms (e.g., Google, Apple). When you do so, we receive basic profile information from the respective provider, which may include your name, email address, friends list, profile picture, and other public data.

We use this information only for the purposes described in this Privacy Notice or as otherwise disclosed on our Services. We do not control how your third-party social media provider collects or uses your data. We encourage you to review their privacy notices to understand how your personal information is handled and how to manage your privacy settings on those platforms.

---

8. Is Your Information Transferred Internationally?

In Short: Yes, we may transfer, store, and process your personal information in countries outside your country of residence, including the United States and Belgium.

Our primary servers are located in **Belgium**. If you access our Services from outside Belgium, please note that your information may be transferred to and processed in Belgium, the United States, or other countries by us or our service providers (as described in **"When and With Whom Do We Share Your Personal Information?"**).

For EEA, UK, and Swiss Residents

These countries may not offer the same level of data protection as your home jurisdiction. However, we implement appropriate safeguards to ensure that your personal information remains protected under applicable laws, including:

Standard Contractual Clauses

We use the **European Commission's Standard Contractual Clauses (SCCs)** for data transfers from the European Economic Area (EEA), the UK, and Switzerland. These clauses contractually require recipients to protect your personal information in compliance with

European data protection standards. Our Data Processing Agreements that include SCCs are available here:
https://firebase.google.com/terms/data-processing-terms

We have also implemented equivalent safeguards with our third-party providers and partners. More details are available upon request.

Data Privacy Framework Certifications

We and certain subsidiaries, including **Google LLC** and **Google Ireland Limited**, comply with:

- The **EU-U.S. Data Privacy Framework (DPF)**
- The **UK Extension to the EU-U.S. DPF**
- The **Swiss-U.S. DPF**

These frameworks are governed by the U.S. Department of Commerce for the secure processing of personal data transferred from the EU, UK (including Gibraltar), and Switzerland. In case of a conflict between this Privacy Notice and the Data Privacy Framework Principles, the Principles shall apply.

You can learn more about the Data Privacy Framework and view our certification at:
https://www.dataprivacyframework.gov/participants

Additional Information Regarding Data Privacy Framework Compliance

In accordance with the **EU-U.S. Data Privacy Framework**, **UK Extension to the EU-U.S. Data Privacy Framework**, and the **Swiss-U.S. Data Privacy Framework**, individuals in the EU, UK, and Switzerland have specific rights concerning the personal information we maintain about them in the United States.

Your Rights Under the Data Privacy Framework

You have the right to:

- Confirm whether we hold personal information about you in the United States.
- Access, correct, amend, or delete that information.

To exercise these rights, please contact us at **hello@intoclimb.com**. We will respond within a reasonable timeframe to all requests, including data deletion where applicable.

If we transfer your personal information to a third-party agent in the United States and that agent processes your information in violation of the Data Privacy Framework Principles, we remain liable unless we can demonstrate that we are not responsible for the event that caused the damage.

We will also provide:

- **An opt-out mechanism** before sharing your personal information with third parties (excluding our agents), or before using it for a materially different purpose than originally collected or authorized.
- **An opt-in mechanism** before sharing any **sensitive personal data** under the same conditions.

To request a limitation on how your personal information is used or disclosed, please send a written request to **hello@intoclimb.com**.

Handling Complaints and Dispute Resolution

We are committed to resolving any complaints related to our handling of your personal data under the Data Privacy Framework.

If you are a resident of the EU, UK, or Switzerland and have a concern or complaint, please contact us first at **hello@intoclimb.com**. If we do not respond in a timely manner or fail to address your concern to your satisfaction, we will cooperate with the following independent authorities:

- **EU Data Protection Authorities (DPAs)**
- **UK Information Commissioner's Office (ICO)**
- **Gibraltar Regulatory Authority (GRA)**
- **Swiss Federal Data Protection and Information Commissioner (FDPIC)**

We agree to comply with the guidance and decisions issued by these authorities in resolving your complaint.

In certain cases, if your issue remains unresolved, you may invoke **binding arbitration** as a last-resort mechanism for specific residual claims.

Enforcement and Government Requests

We are subject to the investigatory and enforcement powers of the **U.S. Federal Trade Commission (FTC)**. We may be required to disclose personal information in response to lawful requests by public authorities, including to meet **national security** or **law enforcement** requirements.

Further Information on Our Data Handling Practices

To learn more about how we process and protect your personal information, we recommend reviewing the following sections of this Privacy Notice:

- **What Information Do We Collect?** – Understand what types of personal information we collect.
- **How Do We Process Your Information?** – Learn about the purposes for which your data is used.

- **When and With Whom Do We Share Your Personal Information?** – See the categories of third parties with whom we may share your data.
- **What Are Your Privacy Rights?** – Learn more about how you can exercise your privacy rights.

Use of Google Firebase and Google Cloud Services

Our backend infrastructure relies on **Google Firebase** and related **Google Cloud** services for data processing and service delivery. Google LLC (or Google Ireland Limited, for users in the EU) is certified under the:

- **EU-U.S. Data Privacy Framework**
- **Swiss-U.S. Data Privacy Framework**
- **UK Extension to the EU-U.S. Data Privacy Framework**

These certifications offer appropriate safeguards for transferring personal data from the **EEA**, **Switzerland**, and the **UK** to the U.S. Google's participation includes adherence to the **Standard Contractual Clauses (SCCs)** and compliance with relevant data protection principles recognized by European and UK regulators.

Independent Recourse and Enforcement

Users in the EU, UK, and Switzerland who have privacy concerns can seek resolution via:

- **Independent dispute resolution mechanisms** in the U.S.
- **Their respective Data Protection Authorities (DPAs, ICO, GRA, FDPIC)**

Google is also subject to **FTC enforcement** in the United States to ensure ongoing compliance with these frameworks.

Your Rights and Control Over Your Data

You maintain full control over your personal data, including rights to:

- Access
- Correction
- Deletion
- Objection to processing

These rights are granted under applicable data protection laws and supported by our partners' data policies.

We encourage users to review **Google's Privacy Policy** and **Data Processing Terms** for further details on how data is processed and protected:

- Google Privacy Policy
- Google Data Processing Terms

9. HOW LONG DO WE KEEP YOUR INFORMATION?

In Short: We retain your personal information only for as long as necessary to fulfill the purposes outlined in this Privacy Notice, unless a longer retention period is required or permitted by law.

We will retain your personal data only for as long as needed to fulfill the purposes described in this Privacy Notice, or as otherwise required by applicable laws (e.g., tax, accounting, or other legal obligations). No purpose in this notice will require us to keep your personal information longer than the duration of your account's existence.

When there is no ongoing legitimate business need to process your data, we will either delete it or anonymize it. If deletion is not possible (e.g., the data is stored in backups), we will securely store and isolate your personal information from further processing until deletion becomes feasible.

---

10. HOW DO WE KEEP YOUR INFORMATION SAFE?

In Short: We implement a range of technical and organizational safeguards to protect your personal information.

We have implemented appropriate technical and organizational security measures to help protect the personal information we process. These measures are designed to prevent unauthorized access, disclosure, alteration, or destruction of your data.

Despite our efforts, no data transmission over the Internet or electronic storage system can be guaranteed to be 100% secure. As such, we cannot guarantee that hackers, cybercriminals, or other unauthorized actors will not be able to bypass our security. You are responsible for accessing our services through a secure environment and transmitting data at your own risk.

---

11. DO WE COLLECT INFORMATION FROM MINORS?

Our services are intended for individuals aged 13 and above. If you are under the age of digital consent in your country (usually between 13 and 16), you must have permission from your parent or legal guardian to use our services.

We do not knowingly collect personal information from children under the age of 13. If we discover that we have unintentionally collected such information, we will take steps to delete it promptly. Parents or guardians who believe we may have collected information from their child can contact us at **hello@intoclimb.com**.

---

12. WHAT ARE YOUR PRIVACY RIGHTS?

In Short: Depending on your location, you may have rights that give you greater access to and control over your personal data.

If you reside in jurisdictions such as the **European Economic Area (EEA)**, **United Kingdom (UK)**, **Switzerland**, **Canada**, or certain U.S. states, you may be entitled to the following rights under applicable data protection laws:

- The right to request access to and obtain a copy of your personal data.
- The right to request correction or deletion of your personal information.
- The right to restrict or object to the processing of your data.
- The right to data portability (if applicable).
- The right not to be subject to automated decision-making with significant effects.

If we use automated decision-making, we will notify you, explain how the decision was made, and provide a simple process to request human review.

You can exercise these rights by contacting us at **hello@intoclimb.com**. We will review and respond to your request in accordance with applicable laws.

If you are in the EEA or UK, and believe we are unlawfully processing your personal information, you have the right to file a complaint with your local data protection authority.

If you are in Switzerland, you may contact the **Federal Data Protection and Information Commissioner (FDPIC)**.

Withdrawing Your Consent

If we are processing your data based on your consent (explicit or implied, as permitted by law), you may withdraw that consent at any time by contacting us at **hello@intoclimb.com**.

Note: Withdrawal of consent does not affect the legality of prior processing, nor does it affect processing based on legal grounds other than consent.

Managing Your Account Information

To review or update your personal data or close your account:

- Log into your account settings to update your profile or request account termination.

Upon receiving your request, we will deactivate or delete your account and remove your data from our active systems. However, we may retain certain information for purposes such as fraud prevention, troubleshooting, legal compliance, or enforcing our terms.

For further questions regarding your privacy rights, contact us at **hello@intoclimb.com**.

13. CONTROLS FOR DO-NOT-TRACK (DNT) FEATURES

In Short: We currently do not respond to DNT signals, as there is no recognized industry standard.

Some web browsers, mobile operating systems, and mobile apps include a “Do-Not-Track” (DNT) feature that allows you to signal your preference not to have your online browsing activities tracked. However, because no uniform standard for recognizing or honoring DNT signals has been finalized, **we do not currently respond to browser-based DNT signals or other similar mechanisms**.

If an industry standard for online tracking is established in the future that we are required to follow, we will update this Privacy Notice to reflect that practice.

Under California law, we are required to disclose our response to DNT signals. At this time, due to the absence of a recognized standard, **we do not respond to DNT signals.**

---

14. DO UNITED STATES RESIDENTS HAVE SPECIFIC PRIVACY RIGHTS?

In Short: Residents of certain U.S. states may have specific privacy rights regarding access to, correction of, or deletion of their personal information, as well as the right to withdraw consent.

If you reside in one of the following U.S. states: **California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah**, or **Virginia**, you may be entitled under state law to:

- Request access to and receive details about the personal information we have collected about you.
- Correct inaccuracies in your personal information.
- Obtain a copy of your personal information.
- Delete your personal information.
- Withdraw consent for our processing of your personal information (where applicable).

These rights may be subject to limitations under applicable state laws. More details on the types of personal information we collect are outlined below.

Categories of Personal Information Collected (Past 12 Months)

The table below outlines the categories of personal information we **have collected** in the past twelve (12) months. This does not necessarily reflect all information collected from you, but rather the categories relevant to our operations. For full details, see **Section: WHAT INFORMATION DO WE COLLECT?**

Category	Examples	Collected
A. Identifiers	Name, alias, postal address, phone number, email address, online identifier, IP address, account name, etc.	✅ Yes
B. Personal information under California law	Name, contact details, education, employment history, financial info	✅ Yes
C. Protected classification characteristics	Age, gender, race/ethnicity, marital status, national origin	❌ No
D. Commercial information	Purchase history, transactions, payment details	❌ No
E. Biometric information	Fingerprints, voiceprints	❌ No
F. Internet or network activity	Browsing/search history, site interactions	❌ No
G. Geolocation data	Device location	❌ No
H. Audio/visual/sensory data	Images, audio or video recordings from business interactions	❌ No
I. Professional or employment-related info	Job title, work history, qualifications (e.g., if applying for a role)	❌ No
J. Education Information	Student records, directory info	❌ No
K. Inferences	Profiles or summaries based on preferences or behavior	❌ No
L. Sensitive Personal Information	Government IDs, precise geolocation, etc.	❌ No

We may also collect other types of personal information outside the categories listed above, when you interact with us in person, online, by phone, or by mail. This may include:

- Requesting help through our customer support channels
- Participating in customer surveys or contests
- Assisting in the delivery of our Services or responding to your inquiries

Retention of Personal Information

We retain collected personal information as long as necessary to provide our Services or as otherwise required by law.

- **Category A (Identifiers)** – Retained as long as your account remains active
- **Category B (California Customer Records Information)** – Retained as long as your account remains active

---

Sources of Personal Information

To learn more about the sources from which we collect personal information, please see the section titled **"WHAT INFORMATION DO WE COLLECT?"**

Use and Disclosure of Personal Information

To understand how we use your personal information, refer to **"HOW DO WE PROCESS YOUR INFORMATION?"**

Disclosure to Third Parties

We may disclose your personal information to service providers under written contracts, as described in **"WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?"**

We may use personal information for internal business purposes, such as product development or testing. This **does not constitute "selling"** of your personal information.

We have not sold or shared personal information with third parties for commercial purposes in the past twelve (12) months.

However, in the last twelve (12) months, we have disclosed the following categories of personal information to third parties for a business or commercial purpose:

- **Category A: Identifiers**

- **Category B: Personal information under the California Customer Records statute**

For details on the third parties involved, refer to **"WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?"**

Your Rights (U.S. Residents)

Depending on your state of residence, you may have the following rights under applicable U.S. data privacy laws:

- **Right to know** whether we are processing your personal data
- **Right to access** the personal data we hold about you
  Right to correct inaccuracies in your personal data
- **Right to delete** your personal data
- **Right to obtain a copy** of your personal data
- **Right to non-discrimination** for exercising your privacy rights
- **Right to opt out** of:
    - Targeted advertising
    - The sale of personal data
    - Profiling in furtherance of decisions that have legal or similarly significant effects

Additional rights may apply depending on your state:

- **Right to access categories** of personal data being processed (e.g., Minnesota)
- **Right to obtain a list of third-party categories** with whom personal data was shared (e.g., California, Delaware, Maryland)
- **Right to obtain a list of specific third parties** receiving personal data (e.g., Minnesota, Oregon)
- **Right to review and correct profiling** (e.g., Minnesota)
- **Right to limit use/disclosure of sensitive data** (e.g., California)
- **Right to opt out of sensitive data collection** via voice/facial recognition (e.g., Florida)

How to Exercise Your Rights

To exercise any of the above rights, you may:

- Visit: intoclimb.com
- Email us: hello@intoclimb.com
- Refer to the contact information at the bottom of this document

You may also authorize an agent to submit a request on your behalf. We may request proof of this authorization in accordance with applicable laws.

Request Verification

To protect your privacy, we will verify your identity before processing any privacy-related requests. We will use the personal information you provide only for verification purposes.

If you are using an authorized agent, we may request:

- Proof of your identity
- A signed authorization granting the agent permission to act on your behalf

---

Appeals

If we deny your request, you may appeal the decision by emailing us at hello@intoclimb.com. We will provide a written explanation of any action taken or not taken.

If your appeal is denied, you have the right to file a complaint with your state's attorney general.

California "Shine The Light" Law

California Civil Code Section 1798.83, known as the "Shine The Light" law, gives California residents the right to request, once per calendar year and free of charge, information about:

- The categories of personal information (if any) we disclosed to third parties for direct marketing purposes
- The names and addresses of all third parties with whom we shared personal information for such purposes during the immediately preceding calendar year

If you are a California resident and wish to make such a request, please submit it in writing using the contact details provided in the section **"HOW CAN YOU CONTACT US ABOUT THIS NOTICE?"**

---

15. Do We Make Updates to This Notice?

In Short: Yes, we update this Privacy Notice as necessary to comply with applicable laws.

We may update this Privacy Notice periodically. Any changes will be indicated by an updated "Revised" date at the top of this document. If we make material changes, we may notify you by posting a prominent notice or sending you a direct notification.

We encourage you to review this Privacy Notice regularly to stay informed about how we protect your personal information.

---

16. How Can You Contact Us About This Notice?

If you have any questions or comments regarding this Privacy Notice, you can reach us by:

- Email: hello@intoclimb.com

---

17. How Can You Review, Update, or Delete the Data We Collect From You?

Depending on the privacy laws applicable in your country or U.S. state of residence, you may have rights to:

- Access the personal information we collect from you

- Learn how we have processed your information
- Correct inaccuracies
- Request deletion of your personal data
- Limit the use or disclosure of your information
- Withdraw consent to processing of your personal information

These rights may be limited under certain circumstances by law.

To submit a request to review, update, or delete your personal data, please visit: intoclimb.com.