

Privacy Policy

Last Revised: August 30, 2024

This Privacy Policy outlines how iMate ("we," "our," or "us") handles the collection, usage, storage, and potential disclosure ("processing") of your personal information in connection with your interaction with our services ("Services"), which include:

- Accessing our official website or any affiliated webpages linking to this Privacy Policy
- Usage of iMate Browser extension
- Usage of iMate Telegram bot
- Participating in communications with us related to product usage, support, promotional campaigns, or events

Need clarification? This Privacy Policy is designed to help you understand your data privacy rights and options. We take responsibility for determining how your personal data is handled. If you disagree with our data practices, please do not use our Services. For any additional inquiries, reach out to us at support@imate.solutions.

Key Takeaways

Below is a summary of the main provisions covered in this Privacy Policy. For detailed explanations, refer to the corresponding sections or navigate via the table of contents.

What personal data do we collect?

When you interact with our Services, we may gather personal data based on your activity, preferences, and the specific features you use. This can include basic identifiers, interaction logs, or technical details.

Do we handle sensitive data?

We do *not* process any data classified as sensitive under relevant privacy laws (e.g., racial or ethnic origin, political opinions, religious beliefs, health data).

Is data obtained from external sources?

We do not acquire personal information from third-party providers or external platforms.

Why do we process your data?

Your data may be processed to operate and enhance our Services, maintain security, fulfill legal obligations, communicate with you, or for purposes you explicitly consent to.

With whom do we share data, and under what circumstances?

Data may be disclosed under specific lawful conditions and only with selected third parties (e.g., payment processors, compliance authorities).

How do we secure your data?

We implement reasonable technical and organizational safeguards to protect your information. However, no internet-based system is fully immune to breaches. We cannot guarantee total security against cyberattacks, unauthorized access, or malicious misuse.

What rights do you have?

Depending on your jurisdiction, you may have legal rights concerning access, correction, erasure, or restriction of your personal data.

How can you assert your rights?

To exercise your rights, you can submit a formal data request or contact our support team. All requests will be evaluated in line with the applicable privacy regulations.

Want more details?

We encourage you to read the complete Privacy Policy for a thorough understanding of how your data is managed.

1. What data are we collecting

Information You Voluntarily Share With Us

Summary: We collect the personal details you choose to provide.

We gather personally identifiable information when you actively submit it—such as when registering for an account, inquiring about our offerings, engaging in platform activities, or initiating direct communication with us.

Details You Provide:

The specific types of personal data we collect are influenced by how you interact with our platform and the functionalities you choose to use. This may include:

- Full names
- Email addresses
- Job roles or titles
- Communication preferences

Sensitive Data:

We do **not** intentionally collect or process any sensitive or special category personal data (e.g., racial origin, religious beliefs, health status).

Payment Information:

If you make purchases via our Services, we may collect payment-related information, including credit/debit card numbers and associated security codes. This data is processed securely via our third-party payment processor, Paddle and Yoomoney. You can view their privacy practices at their official websites.

Social Login Credentials:

You may be given the option to register or log in using a social media account (e.g., Facebook, Google, LinkedIn). If you use this method, we may retrieve limited profile information from the respective platform. Additional details can be found in the “How we handle social media logins” section of this Privacy Policy.

Please ensure the accuracy and completeness of all information you submit. You are responsible for keeping your information current and must notify us of any updates or corrections.

Information Collected Automatically

Summary: Some data is captured automatically during your interaction with our Services.

When you access our platform, we automatically record certain technical information. This may include non-identifying details such as your device type, browser settings, IP address, and usage patterns. Though this data doesn't directly identify you, it is essential for securing, optimizing, and analyzing the performance of our Services.

We may collect this data using cookies or similar tracking tools.

Examples of Automatically Collected Information Include:

- **Log and Usage Records:**
- Our servers log diagnostic and activity data such as your IP address, browser type, settings, device identifiers, access dates and times, pages visited, file downloads, search actions, and interactions with specific features.
- **Device Information:**
- Depending on the hardware you use to access the Services (e.g., computer, smartphone, or tablet), we may collect device-specific details like application IDs, hardware models, internet service provider (ISP) or mobile carrier, operating system, and configuration data.
- **Location Information:**
- We may obtain data about your location, either general or precise. For example, we may use IP-based geolocation or GPS, depending on your device settings and permissions. You can opt out of location tracking by adjusting your device settings. Disabling location access may limit the functionality of certain Services.

Use of Google APIs

Our handling of any personal data obtained via Google APIs complies with the Google API Services User Data Policy, including the stipulations under its Limited Use guidelines.

2. How are we processing your data

Purpose of Processing Your Information

Brief Overview:

We handle your personal data to deliver, maintain, and enhance our Services; to communicate with you effectively; to ensure security and detect fraud; and to meet our legal obligations. We may also process your data for additional purposes, provided we obtain your explicit consent.

We process your personal data for various legitimate purposes based on how you interact with our platform, including but not limited to the following:

- **Account Registration and Management:**
- Your information may be processed to allow you to register an account, authenticate your credentials, and maintain your user profile in good standing.
- **Customer Support and Communication:**
- We may use your data to address support requests, respond to inquiries, and resolve technical or service-related issues that may arise during your use of the platform.
- **Administrative Notifications:**
- Your personal details may be used to deliver important updates about our Services, including policy amendments, product announcements, and service modifications.
- **Order Fulfillment and Transaction Handling:**
- When you place an order or engage in a transaction, we may process your data to manage billing, delivery, refunds, and any related exchanges.
- **Protection of Vital Interests:**
- In exceptional circumstances, we may process your data when necessary to safeguard an individual's essential interests—for example, to prevent injury or protect someone's well-being.

3. What legal grounds are we adhering to process your data

Summary:

We handle your personal data only when it is justified by a legitimate legal basis under applicable law. This may include your explicit consent, legal compliance, contract fulfillment, protection of vital interests, or the pursuit of our legitimate business operations.

For Individuals Located in the European Union or the United Kingdom

If you reside within the EU or the UK, the General Data Protection Regulation (GDPR) and UK GDPR require us to disclose the lawful bases upon which we rely to process your personal data. These may include:

- **Consent:**
- We may use your personal data when you have clearly permitted us to do so for a specific purpose. You have the right to withdraw your consent at any time. Learn more about how to withdraw your consent.
- **Contractual Necessity:**

- We may process your information when it is required for the performance of a contract with you, or to take steps at your request before entering into such a contract.
- **Legal Compliance:**
- Your personal data may be processed if necessary for us to comply with a legal obligation, such as cooperating with government investigations, defending our legal rights, or complying with judicial proceedings.
- **Vital Interests:**
- We may process your data when it is necessary to protect your vital interests or those of another individual, particularly in emergency situations where safety is at risk.
- **Legitimate Interests:**
- In some cases, we may process your information to serve our legitimate business purposes, provided such interests are not overridden by your fundamental rights and liberties.

For Users Residing in Canada

If you are a Canadian resident, we may process your personal data with your express consent, or in some cases, with your implied consent depending on the nature of the interaction. Consent can be revoked at any time.

In limited circumstances, Canadian law may permit us to process your data without obtaining consent, such as when:

- Collection is clearly in the individual's interest and consent cannot be obtained promptly
- It is required for detecting or preventing fraud or for legal investigations
- It occurs as part of a business transaction under specified legal conditions
- It pertains to an insurance-related claim and involves a witness statement
- It is necessary to identify an individual who is injured, ill, or deceased and to contact next of kin
- There are valid reasons to believe the individual has been or may be subject to financial abuse
- Obtaining consent would compromise the accuracy or availability of the data needed for investigating legal breaches
- Disclosure is mandated by a court order, subpoena, or legal process
- The data was created by an individual in a professional capacity and is consistent with the context of its creation
- It is used exclusively for journalistic, artistic, or literary activities
- The information is publicly available and falls under the categories specified by applicable regulations

4. Disclosure of your personal data: when and with whom

Summary:

We may disclose your personal data under specific circumstances outlined below and/or to selected third parties.

There may be instances where sharing your personal information is necessary, including but not limited to the following:

- **Corporate Transactions:**

- Your data may be disclosed or transferred as part of discussions or completion of a corporate transaction such as a merger, acquisition, asset sale, financing arrangement, or in the context of a transfer of all or part of our business to another organization.

5. Use of cookies and similar tracking technologies

Summary:

We may employ cookies and comparable tracking tools to collect and retain your information.

When you engage with our Services, we can select third-party partners that may use various tracking mechanisms—such as cookies, pixels, and web beacons—to gather data. These technologies serve multiple purposes: maintaining platform security, preventing system malfunctions, troubleshooting bugs, preserving your settings, and supporting essential site operations.

Additionally, we allow certain third parties and service providers to implement tracking tools within our Services to conduct analytics and support advertising efforts. These technologies help tailor promotional content to your interests, manage ad placement, and may include reminders for abandoned shopping carts based on your communication preferences. The content you see—either on our Services or external websites—may reflect interests derived from data collected via these tools.

Where applicable U.S. state laws classify these practices as a “sale” or “sharing” of personal data (including targeted advertising), you may opt out by submitting a request as outlined in the section titled “Do United States residents have specific privacy rights?”

Detailed information about our use of cookies and how you can manage or disable certain types of tracking can be found in our section “Use of cookies and similar tracking technologies”.

Use of Google Analytics:

We may use Google Analytics to better understand user behavior on our platform. This may include enabling features such as:

- Google Analytics Remarketing
- Display Network Impression Reporting
- Demographics and Interests Reporting

To opt out of Google Analytics tracking across our Services, visit:

<https://tools.google.com/dlpage/gaoptout>.

You can also manage ad settings via your browser, mobile app preferences, or by visiting the following resources:

- <http://optout.networkadvertising.org/>
- <http://www.networkadvertising.org/mobile-choice>

For more on how Google manages personal data, refer to the Google Privacy & Terms page.

6. Use of artificial intelligence technologies

Overview:

Our Services include features and tools powered by artificial intelligence (AI), machine learning, and related technologies.

To enhance user experience and deliver cutting-edge functionality, we incorporate AI-driven components into our offerings ("AI Tools"). These elements are governed by the terms described in this Privacy Policy and are integrated as part of your use of our Services.

Integration of AI Solutions

We collaborate with third-party providers ("AI Partners")—including but not limited to OpenAI — to deliver AI functionalities. When you use these AI Tools, your inputs, outputs, and associated personal data may be transmitted to and processed by these AI Partners to support your use of the feature. This data processing is conducted in accordance with the applicable legal bases outlined in the section titled **"What legal grounds are we adhering to process your data"**

It is your responsibility to ensure your usage complies with the respective terms of service and acceptable use policies of each AI Partner.

Scope of Our AI Tools

Our AI Tools are currently deployed to support functionalities such as:

- Language comprehension and generation
- Advanced algorithmic task handling

Data Handling and Protection

Any personal data processed via our AI-enabled components is managed securely, in accordance with the principles set forth in this Privacy Policy and our contractual arrangements with technology providers. These measures are in place to uphold your privacy and maintain the integrity of your information throughout the AI interaction lifecycle.

7. How we manage social media logins

Summary: If you opt to sign up for or access our Services using a social media account, we may obtain certain personal details from that account.

Our platform enables users to register or authenticate using credentials from third-party social networking platforms (such as Facebook, Google, LinkedIn etc). If you choose to utilize this method, we may collect specific data associated with your profile from the respective provider. The exact information shared depends on the settings of your social media account and the permissions granted but may typically include your full name, email address, contact list, profile image, and other publicly available profile details.

We will handle any such data in accordance with this Privacy Policy and for the purposes explicitly stated here or elsewhere within the Services where applicable. However, please note that we do not influence or take responsibility for how your social media provider processes your personal information. We encourage you to review the privacy policies of those platforms to understand how they manage your data and what options are available for managing your privacy settings.

8. How long we retain your data

Summary: Your personal information is retained only as long as necessary to fulfill the purposes stated in this Privacy Policy, unless a longer period is legally required.

We store your personal data only for as long as is needed to meet the objectives detailed in this Privacy Policy, unless a longer retention timeframe is required or permitted under applicable laws (such as obligations related to taxation, accounting, or regulatory compliance). None of the purposes described herein require that your personal data be held beyond the duration of your active user account with us.

When we no longer have a legitimate business reason to process your information, we will remove or anonymize the data. If immediate deletion is not technically feasible (e.g., due to the information being contained in system backups), we will securely store and isolate it from any further processing until deletion becomes possible.

9. How we safeguard your information

Summary: We use a combination of organizational and technical safeguards to help secure your personal information.

We take data security seriously and have implemented appropriate administrative, technical, and physical controls to protect your personal information from unauthorized access, alteration, disclosure, or destruction. That said, no internet-based data transmission or storage method is ever completely secure, and we cannot guarantee absolute protection against breaches or unauthorized access by third parties such as hackers or malicious actors.

While we take all reasonable steps to protect your information, any transmission of personal data to or from our Services is done at your own risk. We recommend accessing our Services only through secure and trusted networks.

10. Do we collect data from children?

Summary: We do not intentionally collect or market to individuals under 18 years old.

Our Services are not intended for, nor do we knowingly solicit or collect data from, individuals under the age of 18. We also do not knowingly sell or share personal information from minors. By using the Services, you affirm that you are at least 18 years old or that you are the parent or legal guardian of a minor who is using the Services with your permission.

If we discover that we have inadvertently collected data from a user under the age of 18, we will deactivate the associated account and make reasonable efforts to erase the data from our systems. If you suspect that we may have collected information from a minor, please notify us at **support@imate.solutions**.

11. What are your data protection rights?

Summary: Depending on where you reside—such as certain U.S. states or regions including the European Economic Area (EEA), United Kingdom (UK), Switzerland, and Canada—you may be entitled to rights that grant you greater control over your personal data. You may access, modify, or close your account at your discretion, in accordance with local regulations.

If you reside in jurisdictions such as the EEA, UK, Switzerland, or Canada, you may have rights under local data protection legislation. These rights can include the ability to:

- Request access to your personal data and receive a copy of it;
- Ask for corrections or deletions of inaccurate or unnecessary data;
- Request that we limit the processing of your personal information;
- In certain cases, request that your data be transferred to another party (data portability);
- Object to certain types of processing, including automated decision-making.

To exercise any of these rights, please contact us using the information provided in the section titled “How can you contact us about this Policy” below. All valid requests will be evaluated and processed in accordance with applicable data protection laws.

If you are located in the EEA or UK and believe we are mishandling your personal information, you have the right to file a complaint with your local data protection authority. Swiss residents may reach out to the Federal Data Protection and Information Commissioner for similar concerns.

Withdrawal of Consent:

If we are relying on your consent (either explicit or implied, depending on applicable law) to process your data, you may withdraw that consent at any time. To do so, please contact us using the details in the “**How can you contact us about this Policy**” section or adjust your settings if available.

Please be aware that revoking consent does not affect the legality of prior data processing activities. Additionally, where permitted by law, your information may still be processed on other valid legal bases besides consent.

Marketing Communications:

You may opt out of receiving marketing emails or promotional content at any time by clicking the “unsubscribe” link in our emails or by contacting us directly using the information below. After unsubscribing, you may still receive non-promotional communications from us, such as service notifications, responses to inquiries, or account-related information.

Managing Your Account:

To view, update, or delete your account information, you can:

- Sign in and visit your account settings to update your profile.

If you request that we delete your account, we will remove your account and associated personal information from our active systems. However, we may retain certain details as required to prevent fraud, resolve technical issues, support investigations, enforce our legal terms, or meet legal obligations.

Cookies and Related Technologies:

Most browsers accept cookies automatically by default. You can configure your browser settings to block or remove cookies if you prefer. Note that doing so may affect certain functions or features of the Services.

If you have any inquiries or feedback about your privacy rights, you’re welcome to contact us at **support@imate.solutions**.

12. Controls for Do-Not-Track Features

Many web browsers, mobile operating systems, and applications include a Do-Not-Track (“DNT”) option or setting that you can enable to express your preference that your online browsing data not be monitored or collected. However, there is currently no universally accepted technical standard for recognizing or implementing DNT signals. Accordingly, we do not respond to DNT browser signals or any other automated mechanism that communicates your preference not to be tracked online. Should a standardized method for handling online tracking be established in the future and become mandatory for us, we will update this Privacy Notice to reflect such practice. Under California law, we are required to disclose how we respond to DNT signals from web browsers. Since there is presently no legal or industry standard mandating compliance with DNT signals, we do not honor them at this time.

13. Do United States residents have specific privacy rights?

Summary: If you reside in California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Montana, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Utah, or Virginia, you may possess certain rights related to your personal information. These rights can include requesting access to, obtaining details about, correcting inaccuracies in, receiving a copy of, or deleting personal data we maintain about you. You may also have the ability to withdraw

consent for our processing of your personal information. Please note that some rights may be limited under applicable laws. Additional information is provided below.

Categories of Personal Information We Collect

Within the past twelve (12) months, we have collected personal information in the following categories:

Category	Examples	Collected?
A. Identifiers	Contact details such as your real name, aliases, postal address, telephone number, unique personal identifiers, online identifiers, IP address, email address, and account name	Yes
B. Personal Information under California Customer Records Law	Name, contact info, education, employment history, and financial information	Yes
C. Protected Classification Characteristics	Gender, age, date of birth, race, ethnicity, national origin, marital status, and other demographic data	No
D. Commercial Information	Transaction records, purchase history, financial details, payment info	No
E. Biometric Information	Fingerprints, voiceprints	No
F. Internet or Similar Network Activity	Browsing history, search history, online behavior, interests, interactions with websites, apps, and ads	No
G. Geolocation Data	Device location	No
H. Audio, Electronic, Sensory or Similar Information	Images, audio, video or call recordings related to our business activities	No
I. Professional or Employment Information	Business contact details for service provision, job title, work history, professional	Yes

	qualifications for job	
J. Education Information	Student records, directory information	No
K. Inferences Drawn from Personal Information	Profiles or summaries derived from collected data regarding preferences or characteristics	No
L. Sensitive Personal Information	—	No

Additionally, we may collect other personal data outside these categories when you interact with us in person, online, by phone, or by mail, including:

- Requests for customer support,
- Participation in surveys or contests,
- Facilitation of service delivery and response to inquiries.

Retention and Use of Personal Information

We retain and utilize the personal information collected to provide and improve our services, generally for as long as your account remains active, particularly for categories A, B and I.

Sources of Personal Information

For more details on where we collect your personal information, please refer to the section titled “What data are we collecting”

Use and Sharing of Personal Information

Information on how we use your data is available under “How are we processing your data” We may share your personal data with service providers under written agreements designed to protect your information. More details are found in “Disclosure of your personal data: when and with whom”

We may use your information internally for research and development purposes; such use is not considered the sale of personal information.

In the last twelve (12) months, we have not sold or shared any personal information for commercial purposes and do not intend to do so in the future regarding visitors, users, or consumers.

Your Rights

Certain U.S. state laws grant you rights related to your personal data; however, these rights are subject to limitations and may be denied as permitted by law. These rights include:

- Knowing whether your personal data is being processed,
- Accessing your personal data,
- Correcting inaccuracies,
- Requesting deletion,
- Obtaining copies of data you have provided,
- Protection from discrimination for exercising your rights,
- Opting out of processing for targeted advertising, sale of data, or profiling that results in significant effects.

Depending on your state, additional rights may include:

- Obtaining lists of third parties with whom personal data has been shared,
- Limiting the use and disclosure of sensitive personal data,
- Opting out of collection of sensitive data via voice or facial recognition.

Exercising Your Rights

To exercise your rights, you may submit a data access request via email at **support@imate.solutions** or by using the contact information at the end of this notice.

Some states allow you to authorize an agent to make requests on your behalf. We may require proof of authorization before processing such requests and may deny requests lacking proper authorization.

Request Verification

Upon receiving a request, we will verify your identity using the personal information you provide, or if insufficient, we may ask for additional details for identity verification and security purposes. For requests made through an authorized agent, we may require further verification and a signed authorization letter.

Appeals

If we deny your request, you may appeal by contacting us at **support@imate.solutions**. We will respond in writing with our decision and reasons. If your appeal is denied, you may file a complaint with your state attorney general.

California “Shine the Light” Law

California Civil Code Section 1798.83, known as the “Shine the Light” law, allows California residents to request, once per year and free of charge, information about categories of personal data we disclosed to third parties for direct marketing and the identities of those third parties during the previous calendar year. California residents wishing to make such a request should contact us in writing using the contact details under “How can you contact us about this Policy”

14. Do residents of other regions have specific privacy rights?

Summary: Depending on the country in which you reside, you may have additional privacy rights.

Australia and New Zealand

We collect and handle your personal data in compliance with the requirements and conditions outlined in Australia's Privacy Act 1988 and New Zealand's Privacy Act 2020 (collectively, the "Privacy Acts"). This Privacy Notice fulfills the disclosure obligations mandated by these Privacy Acts, including information about the types of personal data we collect, the sources from which it is obtained, the purposes for which it is used, and any third parties with whom your data may be shared.

If you choose not to provide the personal data necessary for the intended purposes, it could impact our ability to deliver certain services, including:

- Offering the products or services you request;
- Responding to or assisting with your inquiries;
- Managing your account with us;
- Verifying your identity and securing your account.

You have the right, at any time, to request access to or correction of your personal data. To do so, please contact us using the details provided under the section titled "How can you monitor, amend, or delete the data we collect from you"

If you believe your personal information has been handled unlawfully, you may lodge a complaint regarding violations of the Australian Privacy Principles with the Office of the Australian Information Commissioner, or for breaches of the New Zealand Privacy Principles with the Office of the New Zealand Privacy Commissioner.

Republic of South Africa

You may request access to or correction of your personal information at any time by contacting us via the methods detailed in the section "How can you monitor, amend, or delete the data we collect from you"

Should you be dissatisfied with how we resolve any complaints relating to the processing of your personal data, you have the option to escalate your concerns to the relevant regulator:

The Information Regulator (South Africa)

General inquiries: enquiries@inforegulator.org.za

Complaints (using POPIA/PAIA Form 5): PAIAComplaints@inforegulator.org.za & POPIAComplaints@inforegulator.org.za

15. Do we make updates to this Privacy Policy

Summary: Yes, this Privacy Policy may be revised periodically to ensure compliance with applicable laws.

We reserve the right to modify this Privacy Policy as needed. Updates will be reflected by a revised date indicated at the top of this document. For significant changes, we may provide notice either by posting a prominent announcement or by sending you a direct communication. We encourage you to regularly review this Privacy Policy to stay informed about how we manage and protect your personal information.

16. How can you contact us about this Policy

If you have questions, concerns, or comments regarding this Privacy Notice, please contact us by email at support@imate.solutions or in Telegram bot [@iMate_feedback_bot](https://t.me/iMate_feedback_bot)

17. How can you monitor, amend, or delete the data we collect from you

Subject to the laws applicable in your country or U.S. state of residence, you may have the right to request access to the personal data we collect, obtain information regarding how it has been processed, correct any inaccuracies, or request deletion of your personal information. You may also have the right to withdraw consent for the processing of your personal data. These rights may be subject to certain limitations under the law. To exercise any of these rights, please submit a data subject access request using the applicable form or contact method.