



Updated: March 24, 2026

PRIVACY POLICY

Welcome to OutboundSync, Inc. (“we”, “us” or “**OutboundSync**”). We provide a middleware platform that enables the synchronization of data between Sales Engagement Platforms (such as Instantly, Smartlead, EmailBison, and HeyReach) and CRM software (such as HubSpot and Salesforce). We process Personal Data to operate our website <https://outboundsync.com/>, facilitate account access, provide our integration and data-syncing services, maintain platform performance, and improve our Service. By using our website or Services, you agree to the collection and use of information in accordance with this Privacy Policy.

This Privacy Policy should be read alongside and in addition to the Terms of Service. If you are a U.S. resident, additional rights may apply to you. Please refer to sections 9 and 10 for additional information.

This Privacy Policy may be updated to reflect changes in legislation, so please review it now and then. You can always find the most recent version on our website. If you do not agree to the new terms, please stop using the Services.

In this Privacy Policy, “**Personal Data**” includes information such as names, email addresses, CRM contact records, sales engagement metadata, email engagement information (for example, opens, clicks, bounces, reply content), and account configuration details. In certain jurisdictions, this may also be referred to as “Personal Information.”

OutboundSync does not intentionally collect or process Sensitive Data (e.g., biometric data, financial account numbers, government identifiers, or health information) and instructs customers not to sync such information through our platform.

OutboundSync acts primarily as a data processor for our business customers. We process CRM and sales engagement platform data only on behalf of and under the instruction of the customer who connects those systems to OutboundSync. For website visitors and account administrators, OutboundSync acts as a data controller for limited, business-contact-type data (e.g., login information, support communications, marketing preferences).

1. Categories of Personal Data We Collect

(a) **Personal Data You Provide to Us.** Through our Services, we may collect and process Personal Data, including but not limited to:

- **Contact Details.** Includes data such as name, email address, and other business-contact information.
- **Account & Profile Information.** Includes data such as account login credentials, role (e.g., administrator or team member), workspace or organization details, and integration configuration (for example, connected CRM or Sales Engagement Platforms).
- **Communications & Feedback.** Includes data such as content of inquiries, support requests, survey responses, and other communications with us.

- **Other Information You Choose to Provide.** For example, when using beta features, participating in events, or interacting with us online or offline.

(b) Personal Data We Process on Behalf of Our Customers (Data Syncing).

When you connect OutboundSync to your CRM or Sales Engagement Platforms, we process certain data strictly on your behalf and according to your instructions, including:

- **CRM Data.** Such as contacts, companies, deals, owners, lifecycle fields, and other CRM-record information.
- **Sales Engagement Data.** Such as campaign metadata, email sends, opens, clicks, replies, bounces, unsubscribe status, and mailbox-related operational data.

OutboundSync does not intentionally collect or process sensitive data and instructs customers not to sync such information through our platform.

(c) Personal Data We Collect Automatically. When you connect OutboundSync to your CRM or Sales Engagement Platforms, we process certain data strictly on your behalf and according to your instructions, including:

- **Location Information.** When you use our Services, we infer your general location information, for example, by using your Internet Protocol (IP) address. In some jurisdictions, we will ask for your permission before doing so.
- **Device Information.** We receive information about the device and software you use to access our Services, including IP address, web browser type, operating system version, phone carrier and manufacturer, application installations and versions, device identifiers, mobile advertising identifiers, and push notification tokens.
- **Usage Information.** We receive information about your interactions with our Services, such as the content you view, the actions you take, or the features with which you interact when you are using the Services, and the dates and times of your visits.
- **Cookies and Similar Technologies.** Information about your browsing behavior across our Services (see our Cookie section for more details).
- **API and Webhook Logs.** Operational data generated when your connected platforms interact with our Services.

We use technical data to:

- Provide, operate, and maintain our Services.
- Improve, personalize, and expand our Services.
- Understand and analyze how you use our Services.
- Develop new products, services, features, and functionality.
- Communicate with you, either directly or through one of our partners, including for customer service.
- To provide you with updates and other information relating to the Services, and for marketing and promotional purposes.
- Send you emails.
- Find and prevent fraud.

(d) Personal Data We Collect from Third Parties

- **Customer-Provided Data.** Information our business customers send to us through connected CRM or Sales Engagement Platforms, such as contact and company records, deal data, campaign metadata, and email-engagement information.
- **Third-Party Logins.** If you register or sign in using a third-party account (e.g., Google), we may receive basic profile information such as your name and email address.
- **Information from Service Providers.** We may receive limited information from service providers (such as analytics or hosting partners) that help us operate and improve our Services.

In some cases, we need to collect your Personal Data to provide you with our Services. In these cases, if you choose not to provide the requested Personal Data, you may not be able to use our Services.

2. What are the purposes and legal basis for processing your Personal Data?

We process Personal Data for the following purposes and legal bases:

- **Providing our Services.** To create and manage your account, operate the platform, enable integrations, and deliver the Services. This processing is necessary for the performance of our contract with you or based on our legitimate interests in providing the Services.
- **Communicating with you.** To respond to inquiries, provide support, and send essential service notices. This processing is based on our contract with you or our legitimate interests in maintaining the Service.
- **Billing and Transactions.** We process payment and billing information to manage subscriptions, issue invoices, and comply with financial and accounting requirements. This processing is necessary for the performance of our contract and to comply with our legal obligations.
- **Improving and Developing Services.** To analyze usage and maintain the security and performance of the platform. This is based on our legitimate interests in improving and securing the Services.
- **Marketing.** If you subscribe to our updates, we may use your contact details to send newsletters or promotional information. This processing is based on your consent or, in some cases, on our legitimate interest in keeping you informed about our Services. You can opt out at any time.
- **Compliance and Legal Requirements.** We may process Personal Data as required by law, regulation, or court order, and to defend our legal rights. This processing is necessary to comply with our legal obligations and to pursue our legitimate interests in protecting our business.

We do not use customer CRM or synced data to train machine-learning models. When we use your information because we or a third party has a legitimate interest to do so, you may have the right to object to that use.

3. Who We Share Your Data With?

We only share your Personal Data when it is necessary to provide our Services, comply with the law, or protect our users. In particular, we may share your data with:

- **Our team and affiliates.** OutboundSync employees, contractors, and affiliated companies who need access to provide or support the Services.
- **Service providers (sub-processors).** Trusted vendors who help us deliver the Services (such as cloud hosting, payment processing, security, or customer support). These providers process data only under our instructions and with appropriate safeguards.
- **Business customers.** If you are an end user of one of our customers (for example, a bank or other regulated organization), your voiceprints, transcripts, or identifiers are shared with that customer, who controls how the data is used.
- **Legal and regulatory authorities.** Where we believe it is necessary to comply with the law, respond to valid legal requests, prevent fraud or misuse, or protect the rights, safety, and security of OutboundSync, our customers, or the public.
- **In case of a business transaction.** If OutboundSync is involved in a merger, acquisition, financing, or sale of assets, your data may be shared as part of that process.
- **With your consent.** If you ask us to share data or permit us to do so.

We do not sell or rent your Personal Data.

4. Where do we transfer your data to?

OutboundSync is a U.S.-based company, but we provide Services globally. This means that your Personal Data may be transferred to and processed in countries other than where you live. For example, our Services are hosted in the United States and European Union, and we may share data with trusted service providers in those regions to help us operate securely and efficiently.

Typical transfers include:

- **Cloud hosting and storage.** Used to run and secure our platform
- **Connected platforms.** When you choose to connect your CRM or sales engagement platform to our Service, we transfer and sync data with those third-party systems strictly on your instructions and according to your configuration. These platforms act as separate controllers of the data you send to them.
- **Payment processing.** Used to handle billing and payments
- **Analytics and support tools.** Used to improve services and respond to inquiries (e.g., analytics platforms, support channels).

If you are located in the European Economic Area, the United Kingdom, or Switzerland, we ensure that any transfers outside those regions are protected by appropriate safeguards. These may include



Updated: March 24, 2026

the EU Standard Contractual Clauses, the UK Addendum, or transfers to recipients certified under the EU–U.S. Data Privacy Framework, as applicable.

No matter where your data is processed, we apply technical, organizational, and contractual protections to ensure it remains secure and handled in line with this Privacy Policy.

5. Data Retention.

We only keep Personal Data for as long as it is necessary to provide our Services, comply with our legal obligations, resolve disputes, or enforce our agreements. When Personal Data is no longer needed, we take steps to delete it or to keep it in a de-identified form that no longer allows you to be identified.

The specific retention period depends on several factors, including:

- the type of data and the purpose for which it was collected;
- legal and regulatory requirements that may apply; and
- legal and regulatory obligations; and
- the need to maintain records for audit or security.

Where we process Personal Data on behalf of our business customers, we retain that data in accordance with their instructions and applicable law. Retention schedules may differ depending on each customer's configuration and obligations.

6. Cookies and Similar Technologies.

We use cookies and similar technologies (such as pixel tags and SDKs) to collect information about your activity across our Services. A cookie is a small piece of data that the Service saves on your device each time you visit. These technologies allow us to:

- provide secure log-in and essential functionality (strictly necessary cookies);
- measure usage and performance to improve our Services (analytics cookies); and
- show relevant promotions and advertising (advertising cookies).

The categories we currently use on our website are:

- **Preference storage (cookie_consent).** This is our first-party cookie that remembers the choices you make in our cookie banner or settings tool. We store it for up to 12 months. If you reject all cookies, we do not set this cookie.
- **Analytics cookies.** When enabled, we may use Google Analytics (Alphabet, Inc.) to help us understand traffic and usage patterns on our website.
- **Advertising cookies.** When enabled, we may use advertising technologies from Reddit, Inc., LinkedIn Corp. (Microsoft Corp.), X.com (X Corp.), and Google AdWords and YouTube (Alphabet, Inc.) to measure campaigns and support more relevant advertising.

If we add a new analytics or advertising provider to our tag manager setup, we will update this Privacy Policy and our consent experience before using that provider on the website.

If you are located in the European Economic Area, the United Kingdom, or Switzerland, we will only use non-essential cookies (such as analytics or advertising cookies) if you give us your consent through our cookie banner or settings tool. You can change or withdraw your consent at any time.

You can accept, reject, or manage these cookies through the banner when it appears, and you can revisit your choices at any time using the **Manage cookies** link in the footer. If you use the **Clear cookies** control, we will remove the same-origin browser cookies we can access and reset your consent state. Some third-party or HttpOnly cookies may require your browser controls to clear them fully.

If you are located in the United States, certain state privacy laws (such as the California Consumer Privacy Act) may give you the right to opt out of the use of cookies for cross-context behavioral advertising. Please see the U.S. Resident section below for more details.

You can also control cookies by adjusting your browser settings.

7. Children's rights

Our Services are not intended for or directed at children under the age of 18, and OutboundSync does not knowingly collect, store, or process Personal Data from children under the age of 18.

If you are under the age of 18, you are not permitted to submit any Personal Data to us for any Service. If we become aware that we have inadvertently received Personal Data from a child under the age of 18, we will delete that information from our records. If you believe we may have inadvertently processed such Personal Data, please contact us at privacy@outboundsync.com.

8. Your Rights.

Depending on where you live, you may have different rights over your Personal Data. You can exercise your rights by contacting us (see "**Contact Us**" below). We may need to verify your identity before fulfilling your request. Please note that some rights may not apply in all situations, and legal exceptions may apply.

(a) Rights for EU/UK/EEA Residents

If you are located in the European Economic Area, Switzerland, or the United Kingdom, you have the following rights under the GDPR/UK GDPR:

- **Access.** Request confirmation whether we process your Personal Data and obtain a copy.
- **Correction.** Request correction of inaccurate or incomplete Personal Data.
- **Deletion.** Request deletion of your Personal Data, or anonymization where deletion is not possible.
- **Restriction/Objection.** Request that we stop or limit processing of your Personal Data.
- **Portability.** Request transfer of your Personal Data to another provider in a structured, machine-readable format.
- **Withdraw consent.** Withdraw consent at any time, without affecting prior lawful processing.
- **Lodge a complaint.** File a complaint with your local data protection authority.

(b) Rights for U.S. Residents



Updated: March 24, 2026

Some U.S. states provide privacy rights, including rights to access, delete, or opt out of certain types of data sharing.

(c) California Residents (CCPA/CPRA)

If you are a California resident, you have additional rights under the California Consumer Privacy Act (as amended by the CPRA):

- **Right to Know.** Request details about the categories and specific pieces of Personal Data we collect, use, and disclose.
- **Right to Delete.** Request deletion of your Personal Data, subject to legal exceptions.
- **Right to Correct.** Request correction of inaccurate Personal Data.
- **Right to Opt Out of Sale/Sharing.** Opt out of the “sale” or “sharing” of your Personal Data for targeted advertising.
- **Right to Non-Discrimination.** Exercise your rights without discrimination in terms of price or service.

You can exercise these rights by contacting us directly at privacy@outboundsync.com.

9. U.S. Residents.

Residents of certain U.S. states, including California, Colorado, Connecticut, Utah, Virginia, Oregon, Montana, and Texas, have additional privacy rights under state laws. These rights are in addition to those described in section 9 (“Your Rights”).

(a) Sale and Sharing of Personal Information. We do not sell Personal Information. However, some of our use of cookies and advertising tools may be considered “sharing” or “selling” of Personal Information for cross-context behavioral advertising or targeted advertising under U.S. state privacy laws. You can opt out of this activity at any time by:

- Adjusting your cookie preferences through our cookie banner.
- Enabling the **Global Privacy Control (GPC)** signal in your browser, which we honor.

(b) Categories of Data Potentially Shared for Targeted Advertising.

- Online identifiers such as IP addresses, device identifiers, or cookie IDs.
- Usage data, such as interactions with our website or ads.

These categories may be shared with advertising vendors (such as analytics providers, affiliate marketing companies, or tracking technology providers) in order to deliver or measure advertising. We do not knowingly sell or share Personal Information of individuals under the age of 18.

(c) Do Not Track. Our websites and Services are not designed to respond to browser “Do Not Track” signals. We do, however, respect Global Privacy Control (GPC) signals where applicable.

10. Security of Your Personal Data.

We use reasonable and appropriate technical, organizational, and administrative measures to protect Personal Data from unauthorized access, alteration, disclosure, or destruction. These measures may include encryption, firewalls, secure hosting facilities, and strict access controls. If, despite these



Updated: March 24, 2026

safeguards, we become aware of a security incident that is likely to affect your privacy, we will notify you as soon as reasonably possible and in accordance with applicable law.

11. Contact Us

If you have any questions, feel free to contact us at privacy@outboundsync.com.