

Privacy Policy

How LeadFlow Local collects, uses, shares, protects, and retains personal data across its business operations and AI-enabled marketing services.

EFFECTIVE DATE 27 August 2026	LAST UPDATED 27 August 2026
PRIVACY CONTACT <u>contact@leadflow-local.com</u>	

Privacy at a glance

01

We do not sell personal data to data brokers or trade it as a standalone commercial product.

02

Business clients generally control how their customer data is used; LeadFlow handles the agreed technical implementation and support.

03

Analytics and similar non-essential technologies are activated only after the required consent.

04

We minimise identifiable data in AI-assisted workflows and do not use AI alone for legal or similarly significant decisions.

05

Where we access a client-controlled system, we seek to use the minimum access reasonably necessary and end access when it is no longer needed.

Privacy requests can be sent to contact@leadflow-local.com.

CLIENT-CONTROLLED SYSTEMS For many projects, the client chooses the customer relationship, purpose, recipients, and ongoing use. LeadFlow configures and supports the system within that scope. Detailed processor terms are set out in the DPA.

This Policy is a transparency notice; it does not replace a client's own privacy notice or the contractual DPA that applies when LeadFlow processes Customer Personal Data on a client's behalf.

CURRENT FRAMEWORK

Applicable law depends on the person, location, activity, and role. Relevant frameworks include Armenia's Law on Protection of Personal Data (HO-49-N, as amended), Vietnam's Law No. 91/2025/QH15 and implementing rules, and the GDPR only where its territorial scope applies.

01 Who we are and how to contact us

LeadFlow Local LLC is a limited liability company registered in the Republic of Armenia. We provide AI-enabled marketing, websites and landing pages, lead generation, CRM and follow-up systems, advertising support, analytics, automation, and related digital services for business customers in Vietnam and other markets.

ARMENIAN REGISTERED NAME**ԼԻԴՖլՈՒԼ ԼՈՔՎԼ ՍՊԸ****REGISTRATION NUMBER****999.110.1593802****TAXPAYER ID****08327707****REGISTERED ADDRESS****Armenia, Yerevan, Arabkir, Adontsi St. 4/3, 0014****PRIVACY EMAIL****contact@leadflow-local.com****WEBSITE****<https://leadflow-local.com/>**

In this Policy, LeadFlow Local, Company, we, us, and our mean LeadFlow Local LLC. You means an individual whose personal data we process.

02 Scope and our role

This Policy applies to personal data processed through our website, inquiry and onboarding forms, client administration, contracts, billing, support, business communications, campaign pages, lead forms, booking pages, chat tools, CRM systems, advertising accounts, analytics, and automation workflows used in connection with our Services.

For our own website, sales, client administration, billing, security, legal compliance, service management, and direct business communications, we generally decide why and how personal data is processed and act in the controller or equivalent determining role under applicable law.

For many client projects, the business client determines why its customer data is used, which individuals or eligibility rules apply, the purposes and business rules for communications, and whether a configured system remains in operation. Within that agreed scope and subject to applicable law, LeadFlow generally determines routine technical implementation details, such as tooling, workflow configuration, sequencing, and support methods. LeadFlow may temporarily access or process personal data where reasonably necessary for implementation, testing, troubleshooting, or support.

Where LeadFlow processes Customer Personal Data on a client's behalf, the LeadFlow Local Data Processing Addendum (DPA) governs that processing and forms part of the client agreement. Role labels may differ by jurisdiction, and the parties are treated according to their actual functions and applicable law.

CLIENT PRIVACY NOTICE A client's own privacy notice, consent wording, communication terms, and retention rules may apply to the client's customer relationship. This Policy does not replace those materials and is not itself the commercial contract between LeadFlow and a business client.

03 Personal data we collect

The categories below describe data we may process. We do not collect every category in every project.

Identity and business contact data

Name, business name, job title, email address, phone number, city or approximate location, preferred language, and business social-media or directory profiles.

Client, contract, and account data

Onboarding answers, service requirements, contracts, invoices, payment status, transaction references, authorised users, account identifiers, permissions, and communications.

Campaign and customer data

Contact details, service interests, appointment or booking requests, message content, lead source, CRM entries, review or follow-up status, marketing preferences, and consent or opt-out records where used.

Content and project materials

Brand assets, website content, offers, service descriptions, photos, videos, target-audience information, advertising materials, campaign plans, and performance reports.

Technical, analytics, and advertising data

IP address, device and browser information, cookie or advertising identifiers, referral source, UTM parameters, page views, clicks, form and conversion events, approximate location, and server or security logs.

AI and workflow data

Prompts, draft copy, summaries, content variations, audience or workflow labels, testing results, masked or de-identified examples, performance information, and workflow notes.

04 How we collect personal data

Directly from you when you contact us, submit a form, book a call, sign an agreement, complete onboarding, request support, or otherwise communicate with us.

From business clients when they provide project materials, access permissions, customer records, CRM information, communication instructions, or support requests.

Automatically through cookies, pixels, tags, analytics scripts, server logs, local storage, and similar technologies as described in Section 07.

From hosting, CRM, communications, advertising, analytics, automation, payment, security, and AI service providers used in connection with our work.

From public business sources, such as business websites, public social-media pages, maps, directories, and business listings, where lawful and relevant. Public availability does not create unrestricted permission to use personal data.

05 Why we use data and lawful processing

We process personal data only for defined purposes and where permitted by applicable law. Depending on the activity, this may include processing with consent; processing needed to respond to a request or administer a business relationship where law permits; compliance with law; protection or exercise of legal rights where permitted; processing of public-source data where permitted; another statutory exception; or a client's lawful documented instruction when LeadFlow acts on the client's behalf.

Provide and administer services

EXAMPLES

Onboarding, project delivery, websites and campaigns, CRM and automation setup, reporting, support, account management, invoicing, and contract administration.

Manage leads and communications

EXAMPLES

Responding to requests, routing inquiries, booking appointments, sending permitted service or follow-up messages, and maintaining communication history.

Operate and improve systems

EXAMPLES

Analytics, quality assurance, testing, troubleshooting, security, and service development using LeadFlow-controlled data or anonymised or aggregated information that is no longer personal data.

Advertising and measurement

EXAMPLES

Audience management, attribution, conversion measurement, retargeting, optimisation, and campaign reporting, subject to consent and other legal requirements where applicable.

Protect the business and comply with law

EXAMPLES

Security, fraud prevention, incident response, accounting, tax, record-keeping, regulatory cooperation, and establishing, exercising, or defending legal claims.

Our own business marketing

EXAMPLES

Sending information about LeadFlow services to business contacts where permitted, with a practical opt-out where required.

Consent. Where consent is required, we use or support consent mechanisms designed to be informed, specific to the relevant purpose, and capable of being demonstrated as required by applicable law. Withdrawal of consent does not invalidate processing lawfully completed before withdrawal.

06 Client-controlled systems and communications

Our ordinary delivery model is designed to keep the business client in control of its customer relationship and production systems. Where reasonably practicable, CRM, email, SMS, advertising, booking, and automation functionality is configured in client-controlled Third-Party Platforms rather than a separate LeadFlow-controlled customer database.

The client generally determines or approves the intended audience or eligibility criteria, business purpose, and communication rules for review requests, follow-up, marketing, or similar messages. The client is responsible for ensuring that it may lawfully provide the relevant data and request the processing or communications it instructs us to configure. LeadFlow remains responsible for obligations that apply directly to LeadFlow in its own processing role.

We seek to limit production access to what is reasonably necessary for implementation and support. Where practicable, we use test, synthetic, masked, placeholder, or otherwise limited data for configuration and testing. We do not ordinarily maintain a separate standalone copy of a client's full customer database merely for our independent use.

TECHNICAL SUPPORT Temporary exports, logs, troubleshooting records, or other copies may be created where reasonably necessary to perform or support the Services. Where they contain Customer Personal Data, they remain subject to the DPA.

07 Cookies and analytics

We use cookies and similar technologies to operate, secure, and improve our website. Essential cookies support functions such as security, basic functionality, and remembering privacy choices. They are not disabled through the cookie banner because they are necessary for the requested website functions.

Analytics cookies. With your consent, we use analytics cookies and similar technologies to understand website use and improve performance. Analytics information may include pages visited, interactions, date and approximate duration of a visit, referral source, browser and device information, approximate location derived from an IP address, and website performance or error information.

We do not activate analytics or similar non-essential technologies before the required consent. Closing or ignoring the banner, continuing to browse, or remaining inactive is not treated as consent. Rejecting analytics cookies does not prevent access to ordinary website content and functions.

You may change or withdraw your choice through the Cookie Settings control on our website. Where needed to demonstrate compliance, we may retain a limited record of the choice, such as consent status, timestamp, and notice version.

Analytics providers may process information in other countries. Where applicable law requires transfer safeguards, assessments, authorisations, or other measures for our analytics use, LeadFlow completes the obligations that apply directly to LeadFlow.

COOKIE SETTINGS The website's current implementation is designed so that non-essential analytics technologies covered by consent remain inactive until consent is given, and the choice can be changed later through Cookie Settings.

08 AI-assisted tools and automated processing

We use AI and automation to assist with tasks such as drafting and editing content, summarising project information, generating creative concepts, preparing scripts or templates, classifying or tagging workflow items, identifying technical steps, and analysing campaign or service information.

We apply a risk-based approach to personal data in AI-assisted workflows. Where the task does not require identification, we seek to use placeholders, masked, de-identified, aggregated, or otherwise limited information. Where an AI provider processes Customer Personal Data on a client's behalf, the DPA and Subprocessor terms apply to that processing.

LeadFlow does not use Customer Personal Data to train or fine-tune a general-purpose AI model for LeadFlow's independent purposes. A materially different use would require separate written authorisation and a lawful basis. We may use information anonymised or aggregated so that it no longer constitutes personal data under applicable law for security, service analytics, benchmarking, workflow improvement, and reusable know-how, subject to confidentiality and without attempting re-identification.

HUMAN OVERSIGHT We do not use AI alone to make decisions intended to produce legal or similarly significant effects on an individual. Lead scoring, segmentation, tagging, or qualification is intended to support marketing prioritisation or workflow decisions, not final legal, medical, financial, employment, credit, or insurance decisions.

09 How we share personal data

We disclose personal data only where reasonably necessary for the purposes described in this Policy, a client's lawful instruction, the applicable agreement, or law. Recipients may include:

- the business client responsible for the relevant campaign, website, booking page, lead form, CRM, review workflow, or customer relationship;
- hosting, cloud, CRM, email, SMS, messaging, analytics, automation, security, payment, accounting, and technical providers;
- advertising and social-media platforms used for delivery, attribution, audience management, retargeting, or optimisation;
- AI service providers used for content generation, analysis, workflow support, or service delivery;
- professional advisers, accountants, lawyers, auditors, insurers, consultants, and compliance advisers;
- public authorities, regulators, courts, law enforcement, or other parties where legally required or necessary to protect rights, safety, or security; and
- a buyer, investor, lender, or successor in connection with a merger, restructuring, financing, sale, or similar business transaction, subject to appropriate confidentiality and legal safeguards.

NO DATA TRADING We do not sell personal data to data brokers or trade it as a standalone commercial product. Sharing with clients and service providers as described above supports service delivery, administration, security, compliance, or other stated purposes.

10 International processing and transfers

LeadFlow Local is registered in Armenia, serves business clients in Vietnam and other markets, and uses international cloud, communications, CRM, analytics, advertising, automation, and AI tools. Personal data may therefore be stored in, transferred to, or accessed from countries outside the country where the individual or client is located, including jurisdictions where LeadFlow or an authorised service provider operates.

International processing is subject to the requirements that apply to the relevant transfer and role. These may include contractual safeguards, transfer or processing assessments, regulatory filings or authorisations, security measures, localisation rules, or other legal requirements. LeadFlow performs obligations imposed directly on LeadFlow and, when acting for a client, provides reasonable information and assistance regarding obligations connected with LeadFlow's processing.

Vietnamese law may treat use of an overseas platform to process personal data collected in Vietnam as a cross-border transfer. Armenian law separately regulates transfers to other states. Where the GDPR applies to a particular processing activity, its transfer rules apply to that activity.

A client authorisation or contract does not replace a mandatory statutory assessment, filing, approval, or other requirement where the law requires one.

11 Retention

We retain personal data only for as long as reasonably necessary for the relevant purpose, client instructions, contractual obligations, legal or accounting requirements, security needs, dispute resolution, or the establishment, exercise, or defence of legal claims. Retention periods can differ by system, category of data, and processing role.

Where LeadFlow processes Customer Personal Data on a client's behalf, retention is ordinarily governed by the client's lawful instructions, the applicable agreement and DPA, and mandatory law. Temporary data obtained for implementation or troubleshooting is removed, returned, anonymised where appropriate, or allowed to expire when it is no longer reasonably necessary, subject to legal holds, security needs, and normal backup cycles.

These obligations do not require LeadFlow to delete data that remains solely inside a client-controlled system after LeadFlow no longer has access to or control over that data. Information anonymised or aggregated so that it no longer constitutes personal data under applicable law may be retained for lawful security, analytics, reporting, benchmarking, and service improvement.

12 Security

We use technical and organisational measures appropriate to the type of data, the systems used, and the level of risk. Depending on the system and risk, measures may include access controls, secure credential-sharing practices, multi-factor authentication where available and appropriate, least-privilege permissions, protected transmission, confidentiality obligations, logging or monitoring provided by relevant platforms, incident procedures, vendor review, and contractual data-protection terms.

When we access a client-controlled production system, we seek to use the minimum level of access reasonably necessary for the task and to discontinue access when it is no longer required.

SHARED RESPONSIBILITY No system is completely secure. Clients and users are also responsible for protecting their devices, credentials, accounts, recovery methods, and access permissions and for promptly reporting suspected unauthorised access connected with our Services.

13 Your rights and choices

Depending on the law that applies and LeadFlow's role, you may have rights to receive information about processing, access personal data, request correction, withdraw consent, request deletion or restriction, object to certain processing, receive a copy or transfer of data where available, opt out of direct marketing, complain to a competent authority, bring a claim, or seek compensation where the law provides.

To make a request, email contact@leadflow-local.com with the subject Privacy Request and describe the data, client, campaign, or system involved. We may request information reasonably necessary to verify identity and protect personal data against unauthorised disclosure.

Where LeadFlow processes the information only on behalf of a business client, that client will normally determine how the request is handled. We may forward the request to the client and will provide reasonable technical assistance where required by applicable law, the DPA, or the relevant agreement.

You may unsubscribe from our own marketing emails using the unsubscribe mechanism provided or by contacting us. Opting out of marketing does not stop service, billing, security, legal, or other transactional communications that are still necessary or permitted.

14 Sensitive data and children

Our ordinary marketing and automation Services are not designed to require health information, biometric data, government identification, payment-card data, children's data, or other specially protected or high-risk personal data.

Our standard Services do not include processing such data unless LeadFlow has agreed in writing and the parties have established the additional lawful authority, notices or consent where required, security measures, access restrictions, retention rules, contractual terms, assessments, and incident procedures required for that processing.

Our own website and Services are intended for businesses and adult audiences and are not directed to children. A client project intentionally involving children or minors requires advance written disclosure to LeadFlow and all safeguards required by applicable law.

15 Data incidents

If we become aware of a personal data incident, we will take reasonable steps to investigate, contain, mitigate, and preserve relevant information. We will make or support notifications required by applicable law and the relevant agreement according to LeadFlow's role in the affected processing.

When LeadFlow processes Customer Personal Data on behalf of a client, the DPA governs incident notice and cooperation. Where a law places a notification obligation directly on LeadFlow, LeadFlow remains responsible for that obligation; where the client is responsible for a notification, LeadFlow provides the information and assistance reasonably available within our role.

16 Updates, language, and interpretation

We may update this Policy to reflect changes in our Services, systems, providers, legal requirements, or business operations. The current version will be posted on our website with a revised Last updated date. Material changes may also be communicated by email, banner, account notice, or another reasonable method where appropriate.

This English version is the original version. Translations may be provided for convenience or local transparency. Where mandatory law requires a different interpretation, language, or disclosure, the mandatory requirement prevails to the extent of the inconsistency.

17 Contact details

Questions, complaints, and privacy requests may be sent to:

ARMENIAN REGISTERED NAME

ԼԻԴՖԼՈՒԼ ԼՈՔԱԼ ՍՊԸ

REGISTRATION NUMBER

999.110.1593802

TAXPAYER ID

08327707

REGISTERED ADDRESS

Armenia, Yerevan, Arabkir, Adontsi St. 4/3, 0014

PRIVACY EMAIL

contact@leadflow-local.com

WEBSITE

<https://leadflow-local.com/>

EFFECTIVE AND LAST UPDATED

27 August 2026

END OF PRIVACY POLICY This document ends here.