

# Data Processing Addendum

Contractual data-processing terms for business clients using LeadFlow Local services that involve Customer Personal Data.

|                                                                                                                    |                                                                                             |
|--------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| <b>EFFECTIVE DATE</b><br><b>27 August 2026</b>                                                                     | <b>VERSION</b><br><b>1.3</b>                                                                |
| <b>PRIVACY CONTACT</b><br><b><u><a href="mailto:contact@leadflow-local.com">contact@leadflow-local.com</a></u></b> | <b>COMPANY</b><br><b>LEADFLOW LOCAL LLC</b>                                                 |
| <b>APPLIES WITH</b><br><b>Terms of Service / accepted Order</b>                                                    | <b>WEBSITE</b><br><b><u><a href="https://leadflow-local.com">leadflow-local.com</a></u></b> |

## Processing at a glance

### 01

The DPA applies automatically when LeadFlow processes Customer Personal Data on the Customer's behalf.

### 02

The Customer generally controls the customer relationship, purposes, recipients, and lawful business instructions.

### 03

LeadFlow limits production access, prefers client-controlled systems, and uses test, masked, or placeholder data where reasonably practicable.

### 04

LeadFlow does not sell Customer Personal Data or use it for independent marketing to the Customer's end customers.

---

**05**

LeadFlow manages the technical provider stack and may use necessary Subprocessors under this DPA, subject to appropriate safeguards and applicable law.

---

**06**

LeadFlow provides practical assistance with incidents, privacy requests, and assessment information within the scope of its processing.

**ONE AGREEMENT** The accepted Order, Terms, this DPA, and documented Customer instructions form the written processing framework. No separate standard DPA signature is ordinarily required unless mandatory law requires a different form.

This DPA is designed to work with the accepted Order and the LeadFlow Local Terms of Service. It applies only to Customer Personal Data processed by LeadFlow on the Customer's behalf.

**ROLE-BASED APPLICATION**

Different privacy laws use different labels. The parties are treated according to their actual functions and the terminology required by the law that applies to the processing.

# 01 Scope and incorporation

This Data Processing Addendum (DPA) forms part of the Agreement between LEADFLOW LOCAL LLC (LeadFlow) and the business customer identified in an accepted Order (Customer). It applies whenever and to the extent LeadFlow processes Customer Personal Data on the Customer's behalf in connection with the Services.

The DPA takes effect automatically when the Customer accepts an Order governed by the LeadFlow Local Terms of Service and the relevant processing begins. The Customer's recorded acceptance of an Order that provides or links to this DPA is intended to constitute written or electronic agreement to this DPA to the fullest extent permitted by applicable law. No separate standard signature is ordinarily required. The parties may nevertheless execute a separate signed amendment or DPA if a particular Customer, project, or mandatory law requires one.

This DPA does not govern personal data LeadFlow processes independently for its own website, sales, billing, account administration, security, legal compliance, or other legitimate business purposes. Customer Personal Data does not fall outside this DPA merely because it appears in a support ticket or technical record; the exclusion applies only where LeadFlow independently determines that separate processing for its own purpose, as described in the Privacy Policy and subject to applicable law.

**WRITTEN PROCESSING TERMS** The Agreement, this DPA, the accepted Order, and documented Customer instructions together form the written framework for Customer Personal Data processing.

---

## 02 Definitions and roles

**Applicable Data Protection Law** means any privacy or personal-data law, as amended, supplemented, or replaced from time to time, that applies to the relevant processing, including, where applicable, the Republic of Armenia Law on Protection of Personal Data (HO-49-N), Vietnam's Law No. 91/2025/QH15 on Personal Data Protection and its implementing rules, and the EU General Data Protection Regulation only when its territorial scope applies.

**Controller** means the party that determines the purposes and relevant means of processing, or the equivalent determining role under Applicable Data Protection Law. **Processor** means a party that processes personal data on behalf of or under the instructions of a Controller, including an authorised person, service provider, or equivalent instructed role under Applicable Data Protection Law.

**Customer Personal Data** means personal data for which the Customer determines the underlying purpose and that LeadFlow processes on the Customer's behalf in connection with the Services under this DPA. **Subprocessor** means a third party engaged by LeadFlow to process Customer Personal Data on LeadFlow's behalf in connection with the Services.

**Personal Data Incident** means a security breach or other personal-data-protection violation involving Customer Personal Data that Applicable Data Protection Law treats as requiring investigation, mitigation, notice, or other action, including accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access.

For Customer Personal Data, the Customer generally acts as Controller or the equivalent determining party and LeadFlow generally acts as Processor or the equivalent instructed party. If the actual facts or mandatory law assign different roles, those roles apply to the relevant processing and the parties will cooperate in good faith to document any material adjustment required by law.

---

## 03 Customer instructions and lawful use

LeadFlow will process Customer Personal Data only as reasonably necessary to provide, secure, maintain, troubleshoot, and support the contracted Services within the scope of the Customer's documented instructions, or as required by law. Documented instructions include the Order, this DPA, configuration choices, authorised support tickets, emails, messages, and other clear written or electronic directions given by an authorised Customer representative.

The Customer determines the underlying business purposes and the decisions only the Customer controls, including which individuals or categories of individuals should receive Customer communications. The Customer is responsible for ensuring that it has the lawful authority, consent, notice, permission, contract, or other processing condition required to collect Customer Personal Data, provide it to LeadFlow, and instruct the relevant processing or communications.

Subject to the Customer's documented purposes, data scope, recipient or eligibility rules, substantive business instructions, the accepted Order, this DPA, and Applicable Data Protection Law, LeadFlow may determine ordinary non-essential technical means and implementation details, including workflow sequencing, configuration methods, internal tools, and vendor choices. LeadFlow will not use that technical discretion to materially change the Customer's underlying processing purpose or expand the agreed Customer Personal Data scope.

If LeadFlow reasonably believes an instruction is unlawful, materially unsafe, outside the agreed scope, or inconsistent with this DPA, LeadFlow may pause the affected processing and ask the Customer to clarify or modify the instruction. LeadFlow is not required to follow an instruction that Applicable Data Protection Law prohibits.

The Customer must not provide or instruct processing of health information, biometric data, government identification, payment-card data, children's data, or other specially protected or high-risk personal data unless LeadFlow has agreed in writing and the additional legal, security, assessment, retention, and contractual requirements for that processing have been addressed.

---

## 04 Processing scope and data minimisation

The subject matter, duration, nature, purposes, data categories, data subjects, recipients, and processing conditions are described in Schedule 1 and may be supplemented by the accepted Order. LeadFlow will process Customer Personal Data only within that documented scope.

Where reasonably practicable, LeadFlow will use client-controlled production systems and the minimum amount of Customer Personal Data needed to perform the task. For implementation, development, testing, and troubleshooting, LeadFlow will seek to use synthetic, masked, pseudonymised, de-identified, placeholder, or otherwise limited data where the task does not require identifiable information.

LeadFlow will not ordinarily create or maintain a separate standalone copy of the Customer's full customer database merely for LeadFlow's independent use. Temporary exports, logs, troubleshooting records, or other copies may be created where reasonably necessary for the Services and remain subject to this DPA.

LeadFlow will not sell Customer Personal Data, trade it as a standalone commercial product, or use it for LeadFlow's independent direct marketing to the Customer's customers or prospects.

---

## 05 Confidentiality and personnel

LeadFlow will limit access to Customer Personal Data to personnel, contractors, and Subprocessors who need access for the Services or related security, legal, or support functions. Persons acting under LeadFlow's authority who access Customer Personal Data must be subject to appropriate confidentiality obligations or a legal duty of confidentiality.

LeadFlow will not intentionally disclose Customer Personal Data to another person except as permitted by this DPA, the Agreement, the Customer's documented instructions, or Applicable Data Protection Law. Confidentiality obligations concerning Customer Personal Data continue for as long as LeadFlow or its Subprocessors retain or can access the data.

---

## 06 Security and access

LeadFlow will maintain technical and organisational safeguards appropriate to the nature of the Customer Personal Data, the Services, and the reasonably foreseeable risks. The baseline measures are described in Schedule 2 and may be supplemented where a particular Order or mandatory law requires additional controls.

LeadFlow will seek to apply least-privilege access and to discontinue production access when it is no longer reasonably required. Where secure account-sharing, access delegation, or multi-factor authentication features are available and appropriate, LeadFlow will use or support those features according to the relevant platform and project context.

No security measure eliminates all risk. The Customer remains responsible for the security of Customer-controlled accounts, devices, recovery methods, users, and permissions except to the extent an Order expressly assigns a particular security function to LeadFlow.

---

## 07 Subprocessors and Third-Party Platforms

The Customer gives LeadFlow general authorisation to engage Subprocessors reasonably necessary to provide the Services, subject to this DPA and Applicable Data Protection Law. LeadFlow may select and change vendors, tools, and technical methods as reasonably necessary for security, performance, compatibility, cost, or service delivery unless an Order expressly requires a particular provider.

LeadFlow will require each Subprocessor that processes Customer Personal Data on LeadFlow's behalf to be bound by appropriate confidentiality and data-protection obligations consistent with LeadFlow's obligations for the processing assigned to that Subprocessor. LeadFlow remains responsible for its contractual obligations under this DPA, subject to the liability provisions of the Agreement.

LeadFlow will make a current list of Subprocessors that process Customer Personal Data available on request and may also publish it on a designated legal page. Where Applicable Data Protection Law requires specific notice, approval, or a right to object to a new Subprocessor, LeadFlow will provide the legally required mechanism. Any objection must be based on reasonable data-protection grounds. If the parties cannot resolve a legally required objection and no commercially reasonable alternative is available, either party may terminate the affected future Service without requiring LeadFlow to discontinue unrelated Services. Any such termination remains subject to the Agreement's payment provisions, including amounts already earned, accrued, or committed before termination.

Third-Party Platforms controlled directly by the Customer are governed by their own terms. To the extent LeadFlow merely accesses a Customer-controlled platform under Customer instructions and does not select the platform as LeadFlow's Subprocessor, the platform is not treated as LeadFlow's Subprocessor solely because LeadFlow provides technical support within it.

---

## 08 International processing and transfers

The Customer authorises LeadFlow to process Customer Personal Data in jurisdictions where LeadFlow or authorised Subprocessors operate, subject to Applicable Data Protection Law and any express data-location restriction in the Order. Unless the Order expressly states a data-residency commitment, LeadFlow does not promise that Customer Personal Data will remain in a particular country.

Each party is responsible for transfer, localisation, assessment, filing, approval, notification, or other international-processing obligations imposed directly on that party by Applicable Data Protection Law. LeadFlow will provide information reasonably available to LeadFlow that the Customer needs to complete an assessment or filing connected with LeadFlow's processing, and LeadFlow will complete obligations imposed directly on LeadFlow in its own role.

Where Armenian law requires an adequate destination or regulatory permission for a transfer, the relevant requirement must be satisfied before the transfer. Where Vietnamese law treats use of an overseas platform or foreign recipient as a cross-border transfer, the responsible party must complete any required transfer-impact assessment, filing, update, or related safeguard. Where the GDPR applies, the transfer mechanisms required by the GDPR apply to that processing.

This DPA provides contractual processing safeguards but does not by itself replace a statutory filing, government approval, transfer-impact assessment, or other mandatory regulatory step.

---

## 09 Data-subject requests

The Customer is generally responsible for determining how to respond to requests from individuals concerning Customer Personal Data, including requests for information, access, correction, deletion, restriction, withdrawal of consent, objection, portability, or other rights available under Applicable Data Protection Law.

If LeadFlow receives a request that primarily concerns Customer Personal Data processed on the Customer's behalf, LeadFlow may direct the individual to the Customer or promptly forward the request to the Customer, unless Applicable Data Protection Law requires LeadFlow to respond directly.

Taking into account the nature of the processing, information available to LeadFlow, and the complexity of the request, LeadFlow will use reasonable efforts to provide required technical assistance without undue delay and in time for the Customer to meet applicable statutory deadlines, where that assistance is required by Applicable Data Protection Law or this DPA.

---

## 10 Personal Data Incidents

LeadFlow will notify the Customer without undue delay after becoming aware of a Personal Data Incident affecting Customer Personal Data processed by LeadFlow or its Subprocessor. LeadFlow may provide information in stages as the investigation develops and will not delay an initial notice solely because all facts are not yet known.

To the extent reasonably available, the notice or follow-up information will describe the nature of the incident, affected data or systems, likely consequences where known, containment or mitigation steps, and a contact point for coordination. LeadFlow will take reasonable measures to contain, investigate, and mitigate the incident within its systems or responsibility.

The Customer is responsible for determining and making notifications to individuals or authorities where the obligation falls on the Customer. LeadFlow will provide reasonable assistance and information within LeadFlow's control. Where Applicable Data Protection Law imposes a notification obligation directly on LeadFlow, LeadFlow remains responsible for that obligation.

Incident communications under this Section do not constitute an admission of fault or liability.

---

## 11 Retention, return, and deletion

LeadFlow will retain Customer Personal Data only for as long as reasonably necessary to provide or support the Services, follow lawful Customer instructions, satisfy legal or security requirements, or resolve disputes, subject to the Agreement and Applicable Data Protection Law.

On termination or a valid Customer instruction, LeadFlow will return, delete, anonymise, or cease active processing of Customer Personal Data under its control as reasonably practicable. Continued retention is limited to data required by law or supported by a separate lawful basis in LeadFlow's independent role for security, compliance, or legal claims. Retained data remains protected, is not used for unrelated Customer-directed processing, and backups may remain only until normal overwrite or deletion.

This Section does not require LeadFlow to delete Customer Personal Data that remains solely in a Customer-controlled system after LeadFlow has returned or removed its own access and no longer controls that data.

---

## 12 Assessments and regulatory assistance

Taking into account the nature of LeadFlow's processing and the information available to LeadFlow, LeadFlow will provide reasonable information and assistance concerning privacy or transfer impact assessments, regulator inquiries, security documentation, and similar obligations that relate directly to LeadFlow's processing of Customer Personal Data.

Ordinary assistance reasonably necessary because of LeadFlow's processing obligations is included as part of the Services. Substantial bespoke compliance projects, preparation of the Customer's broader regulatory filings, legal analysis for the Customer's independent business, or work materially beyond the ordinary scope may require a separate Order or reasonable additional fees, unless the work is required because of LeadFlow's material breach of this DPA or Applicable Data Protection Law.

Nothing in the Agreement prevents LeadFlow from cooperating with a competent regulator or authority where LeadFlow is legally required to do so.

---

## **13 AI-assisted processing and permitted non-personal use**

LeadFlow may use AI systems and AI service providers to perform the Services. Where an AI provider processes Customer Personal Data on LeadFlow's behalf, the provider is subject to the Subprocessor requirements of this DPA to the extent applicable.

Where reasonably practicable, LeadFlow will remove direct identifiers or use placeholders, masked, pseudonymised, de-identified, or aggregated information when the AI task does not require identification.

LeadFlow does not use Customer Personal Data to train or fine-tune a general-purpose AI model for LeadFlow's independent purposes. Any materially different use requires a separate written agreement and a lawful basis and is outside this standard DPA.

LeadFlow may use information anonymised or aggregated so that it no longer constitutes personal data under Applicable Data Protection Law for security, service analytics, benchmarking, quality assurance, workflow improvement, and development of reusable know-how, provided it does not disclose the Customer's Confidential Information and LeadFlow does not attempt re-identification.

---

## 14 Compliance information and audits

On reasonable request, LeadFlow will provide information reasonably necessary to demonstrate compliance with this DPA and the obligations applicable to LeadFlow's processing role, subject to confidentiality, security, legal privilege, third-party restrictions, and protection of other customers' information.

A Customer audit should ordinarily begin with available policies, summaries, questionnaires, certifications, or other documentary information. An onsite or technical audit may be requested only where required by Applicable Data Protection Law or where a material unresolved compliance concern cannot reasonably be addressed through less intrusive information.

Any audit must be proportionate, conducted on reasonable prior notice during normal business hours, subject to confidentiality, designed to avoid unnecessary disruption, and must not expose other customers' data or LeadFlow's unrelated confidential systems. The Customer will bear reasonable audit costs unless the audit identifies a material breach of this DPA by LeadFlow or Applicable Data Protection Law requires another allocation.

---

## 15 Liability

Liability arising out of or relating to this DPA is subject to the exclusions and limitations of liability in the LeadFlow Local Terms of Service, except to the extent Applicable Data Protection Law does not permit the relevant exclusion or limitation.

Nothing in this DPA limits a party's mandatory statutory responsibility to an individual, regulator, or other person where that responsibility cannot lawfully be excluded or limited by contract.

---

## 16 Duration and termination

This DPA begins when it first applies to Customer Personal Data under Section 01 and continues for as long as LeadFlow or a Subprocessor processes Customer Personal Data on the Customer's behalf.

Termination or expiry of an Order ends LeadFlow's authority to perform new processing for that Order except as reasonably necessary for return, deletion, transition, security, dispute resolution, or legal compliance, and only to the extent permitted or required by Applicable Data Protection Law.

Sections concerning confidentiality, security, incidents, deletion, regulatory cooperation, audit, liability, and any provision intended by its nature to continue will survive for as long as relevant Customer Personal Data remains subject to this DPA.

---

## 17 General terms and precedence

For Customer Personal Data processing, this DPA prevails over inconsistent provisions of the Terms or an Order unless a signed amendment expressly identifies and modifies the relevant DPA provision. The Order controls the commercial scope, Services, fees, and project-specific instructions to the extent they do not reduce mandatory data-protection requirements.

The governing law and dispute-resolution provisions of the Terms apply to this DPA, subject to mandatory Data Protection Laws and regulator jurisdiction that apply independently to a particular processing activity.

Internal LeadFlow policies, procedures, security standards, vendor registers, and operational records may support compliance but do not become contractual terms merely because they are referenced or used to perform the Services. LeadFlow may update internal procedures provided the protection required by this DPA and Applicable Data Protection Law is maintained.

If a provision of this DPA is invalid or unenforceable, the remaining provisions remain effective and the affected provision will be adjusted only to the minimum extent necessary to preserve its lawful purpose.

**END OF STANDARD TERMS** Schedules 1 and 2 below form part of this DPA and describe the default processing assignment and baseline security measures.

---

# Schedule 1 - Default processing description

This Schedule provides the standard written processing assignment for ordinary LeadFlow business-client Services. An accepted Order may supplement it. If a project materially exceeds this default scope, the parties should document the additional processing before it begins.

## Subject matter

Processing Customer Personal Data reasonably necessary to implement, configure, test, support, troubleshoot, secure, and deliver the Services described in the accepted Order.

## Grounds / written assignment

The Customer's accepted Order, the Terms, this DPA, and lawful documented Customer instructions together form the written processing assignment. The Customer confirms the lawful authority or processing condition needed to instruct LeadFlow; LeadFlow processes within that assignment and applicable law.

## Duration

For the implementation or service term and any limited support, transition, security, backup, dispute, or legal-retention period permitted by the Agreement and Applicable Data Protection Law.

## Nature / operations

Receiving, accessing, viewing, organising, configuring, storing where necessary, transmitting, routing, structuring, classifying, automating, testing, troubleshooting, supporting, correcting, exporting where necessary, deleting, returning, pseudonymising, de-identifying, or anonymising where appropriate within the agreed Services.

## Purposes

Providing and supporting client-selected CRM, review-request, lead-routing, booking, forms, follow-up, communications, analytics, website, advertising-support, automation, and related technical Services described in the Order.

---

## **Data subjects**

The Customer's customers, prospects and leads; users of Customer systems; Customer personnel and authorised users; and other individuals whose data the Customer lawfully includes in the relevant workflow.

## **Ordinary data categories**

Names; email addresses; phone numbers; business or customer identifiers; service interests; booking or appointment information; communication content or status; CRM records; review-request or follow-up status; lead source; marketing preferences or consent/opt-out records; and technical or workflow metadata reasonably necessary for the Services.

## **Excluded by default**

Health information, biometric data, government identification, payment-card data, children's data, or other specially protected or high-risk personal data unless separately agreed in writing with appropriate safeguards.

## **Recipients**

The Customer and its authorised users; LeadFlow personnel and contractors with a need to know; authorised Subprocessors; Customer-controlled Third-Party Platforms; and competent authorities where disclosure is legally required.

## **Locations**

Jurisdictions where LeadFlow or authorised Subprocessors operate, and Customer-controlled platform locations, subject to applicable transfer, localisation, assessment, filing, and authorisation requirements. No specific data residency is promised unless the Order expressly states one.

## **Instructions**

The Order, this DPA, configuration choices, service settings, authorised support tickets, emails, messages, and other documented directions from an authorised Customer representative.

## **Technical implementation**

Within the documented purposes and instructions, LeadFlow may determine ordinary non-essential technical means, workflow sequencing, configuration methods, internal tools, and Subprocessor choices, subject to this DPA and applicable law.

### **Protection measures**

The baseline protection measures in Schedule 2 apply, together with any additional safeguards expressly required by the Order or Applicable Data Protection Law.

### **Customer authority / conditions**

The Customer is responsible for ensuring that it has any lawful authority, consent, notice, permission, contract, or other processing condition required to collect and use the Customer Personal Data and instruct LeadFlow. LeadFlow processes under the Agreement, this DPA, the Order, and lawful documented Customer instructions.

---

## Schedule 2 - Baseline security measures

The measures below are risk-based baseline commitments. The exact technical implementation may vary by platform and project. LeadFlow may use equivalent or stronger controls and may update internal procedures without reducing the protection required by this DPA or Applicable Data Protection Law.

### Governance and confidentiality

Limit Customer Personal Data access to authorised persons with a service, support, security, or legal need; maintain appropriate confidentiality obligations; and use internal procedures proportionate to the processing risk.

### Access control

Use least-privilege or role-based access where supported; avoid shared access where individual access is reasonably available; remove or discontinue access when no longer required.

### Credentials and authentication

Use secure credential-sharing methods where available; support strong passwords and multi-factor authentication where the relevant platform provides it and the project context makes it appropriate.

### Transmission protection

Use encrypted or otherwise appropriately protected transmission for Customer Personal Data over public networks through the security capabilities of the relevant platform or protocol.

### Data minimisation

Use the minimum data reasonably necessary; prefer test, synthetic, masked, pseudonymised, de-identified, placeholder, or otherwise limited data where identifiable production data is unnecessary.

### System and device security

---

Use device, account, endpoint, software-update, and access safeguards appropriate to the systems through which LeadFlow accesses Customer Personal Data.

### **Logging and monitoring**

Use or rely on relevant platform logs, access records, alerts, or monitoring capabilities where available and appropriate to the risk and Service.

### **Incident handling**

Maintain a process to identify, investigate, contain, mitigate, document, and communicate Personal Data Incidents in accordance with the DPA and Applicable Data Protection Law.

### **Vendor management**

Review Subprocessors and require appropriate confidentiality and data-protection terms for Customer Personal Data within the scope assigned to them.

### **Deletion and access closure**

Return, delete, anonymise where appropriate, or cease active processing of Customer Personal Data as required by the DPA, and close LeadFlow production access when it is no longer reasonably needed.

**DPA CONTACT** Questions about this DPA or Customer Personal Data processing may be sent to [contact@leadflow-local.com](mailto:contact@leadflow-local.com). Standard DPA version 1.3 is effective 27 August 2026.