

# Privacy Policy

Development 360

Last updated: 10 August 2026

Effective: 10 August 2026

## 1. Controller identity and contact details

---

Development 360 ("Development 360", "we", "us") is a customer relationship management ("CRM") platform for real-estate developers. The platform is operated by:

შპს დეველოპმენტ 360 (LLC Development 360)

Identification code: 405871310

Tbilisi, Georgia

Privacy contact: [privacy@development360.ge](mailto:privacy@development360.ge)

This Privacy Policy explains what personal data we handle, why, on what legal basis, who else sees it, and what rights you have. It is written to the Law of Georgia on Personal Data Protection, and follows the standards of the EU General Data Protection Regulation ("GDPR") where those go further.

## 2. Roles of the parties: controller and processor

---

Development 360 is provided to companies. Personal data therefore reaches us in two distinct ways, and our responsibilities differ in each case.

**a) Data we control.** Information about our own business customers and their staff — the people who hold a Development 360 login. We decide why and how this is processed, so we are the **data controller**.

**b) Data we process for a customer.** Everything a customer's team puts into their workspace: their sales leads, buyers, conversations with prospective purchasers, uploaded documents. We hold this **on that company's instructions only**. The developer company is the **data controller**; we are a **data processor**.

If you are a home buyer, an enquirer, or anyone else whose details were entered into a developer's Development 360 workspace, **the developer company — not Development 360 — decides what happens to your data**. Contact that company first. If you cannot identify or reach them, write to us at [privacy@development360.ge](mailto:privacy@development360.ge) and we will route your request to the relevant customer.

### 3. Personal data processed as controller (customers and their personnel)

| Category                     | Examples                                                                                                                                  | How collected                                                                | Purpose                                                   | Legal basis                                    |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|-----------------------------------------------------------|------------------------------------------------|
| Account identity             | Full name, work email, phone number, role (admin, sales lead, agent, marketing), organisation membership, account status                  | Entered by the customer's administrator when inviting a user, or by the user | Creating and securing the account; access control         | Performance of a contract                      |
| Authentication               | Password (stored only as a cryptographic hash by our authentication provider — we never see or store it in readable form), session tokens | On sign-in                                                                   | Authenticating the user; keeping sessions secure          | Performance of a contract                      |
| Support and correspondence   | Messages you send us, the context needed to answer them                                                                                   | When you contact us                                                          | Answering support and contractual queries                 | Legitimate interest; performance of a contract |
| Technical and security logs  | IP address, browser and device type, timestamps, requested URL, request identifier, error traces                                          | Automatically, by our hosting providers and application servers              | Operating the service, diagnosing faults, detecting abuse | Legitimate interest; legal obligation          |
| Billing and contract records | Company name, identification code, contact person, invoices and correspondence                                                            | Provided when contracting                                                    | Invoicing, accounting, statutory record-keeping           | Performance of a contract; legal obligation    |

We do **not** process payment card data. The platform contains no payment processing; invoicing takes place outside the application.

### 4. Personal data processed on behalf of customers

When a customer uses the platform, their team enters and generates data about third parties — mainly prospective and actual property buyers. Depending on how a customer configures their workspace, this can include:

- **Lead records:** name, one or more phone numbers, email address, budget, currency, the project, unit type, number of rooms, floor and area a person is interested in, purchase purpose, lead source, free-text notes, and the history of contact with them (calls, emails, messages, notes, stage changes, timestamps).
- **Conversations:** the content of messages exchanged with a prospective buyer through a messaging channel the customer has connected, together with the sender's display name, username, profile picture and, where the channel provides it, phone number.
- **Buyer and deal records:** buyer name, the unit purchased, price, area, and the payment schedule agreed.
- **Files:** documents a customer's team uploads against a lead or a project — for example draft agreements, price lists or identity documents. We do not inspect the contents of these files; a customer may upload documents

containing sensitive information, and it is that customer's responsibility to have a lawful basis for doing so.

- **Calendar entries** relating to viewings, calls, meetings and tasks.

We process this data **only** to provide the platform to the customer, to keep it secure, and where the customer instructs us. We do not use it to build profiles of buyers, we do not use it for our own marketing, and we do not sell it.

## 5. Messaging channel integrations

A customer may connect messaging channels — Facebook Messenger, Instagram, Telegram, Viber — so that enquiries arrive in the platform. The following consequences apply:

1. **Messages travel through the channel provider.** When a buyer writes to a developer's Facebook Page or Telegram bot, that message passes through Meta's or Telegram's systems under their own privacy terms before reaching us. The same applies in reverse when a sales agent replies.
2. **Contact details come from the channel.** We receive the identifiers the provider supplies, such as a display name, username or profile picture. For Meta channels we may perform a profile lookup to resolve a readable name; this can fail, in which case the contact appears without a name.

Media files attached to inbound messages are referenced at the provider's own address and expire according to that provider's rules; we do not currently re-host them.

## 6. Cookies and local storage

We use **no advertising cookies, no analytics cookies, no tracking pixels and no cross-site tracking whatsoever**. The platform integrates no third-party analytics product. What we do store on your device is strictly operational:

| Name                  | Type                                               | Purpose                                                                                              | Duration                   |
|-----------------------|----------------------------------------------------|------------------------------------------------------------------------------------------------------|----------------------------|
| kv_refresh            | HttpOnly cookie, scoped to the authentication path | Keeps you signed in and lets your session be renewed. Cannot be read by scripts in the browser.      | Until sign-out or expiry   |
| Saved lead filters    | Local storage                                      | Remembers filter sets you saved for the lead list                                                    | Until you clear it         |
| Sound preference      | Local storage                                      | Remembers whether you muted the new-message chime                                                    | Until you clear it         |
| Theme                 | Local storage                                      | Remembers light or dark appearance                                                                   | Until you clear it         |
| Meta connection state | Session storage                                    | Holds which provider you are connecting during a Facebook authorisation, for the length of that flow | Deleted when the flow ends |

Your access token is held **in memory only** and is never written to local storage, which reduces its exposure if a browser extension or script misbehaves.

Because none of the above is used for advertising or profiling, no cookie consent banner is presented; strictly necessary storage does not require consent under Georgian law or the GDPR.

## 7. Recipients and disclosure of personal data

We share data only with the following categories of recipient, and only as needed to run the service:

| Recipient                                                             | Role                                        | What they receive                                                                                   |
|-----------------------------------------------------------------------|---------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Cloud database, storage and authentication provider                   | Processor (sub-processor)                   | Hosts the database, uploaded files and authentication records                                       |
| Application hosting and content delivery provider                     | Processor (sub-processor)                   | Serves the web application and backend; processes request metadata and logs                         |
| Meta Platforms (Facebook, Instagram)                                  | Independent controller for its own platform | Only where a customer connects a Meta channel: message content and the connected Page's identifiers |
| Telegram                                                              | Independent controller for its own platform | Only where a customer connects a Telegram bot: message content and bot identifiers                  |
| Viber                                                                 | Independent controller for its own platform | Only where a customer connects a Viber account: message content and account identifiers             |
| Listing portals, advertising platforms, banks and telephony providers | Independent controllers                     | Only where a customer connects them, and only the data required for that specific integration       |
| Professional advisers, auditors                                       | Controller or processor as applicable       | Where necessary and under confidentiality                                                           |
| Public authorities                                                    | —                                           | Where we are legally compelled, after checking that the request is valid and lawful                 |

Integrations are **off by default**. Nothing is sent to Meta, Telegram, Viber, a listing portal or a bank unless a customer's administrator deliberately connects that channel.

We do not sell personal data. We do not share it for behavioural advertising. We have never received a government access request of the kind that would require disclosure here.

## 8. International data transfers

Our infrastructure providers may store and process data outside Georgia, including in the European Union and the United States. Where data leaves Georgia we rely on the transfer grounds available under Georgian data protection law and, where the GDPR applies, on appropriate safeguards such as the European Commission's Standard Contractual Clauses together with our providers' own transfer frameworks. You may request details of the safeguards applying to a specific transfer by writing to [privacy@development360.ge](mailto:privacy@development360.ge).

## 9. Data retention

- **Account data:** for as long as the account exists, and for up to 12 months afterwards to handle disputes and reinstatement requests.

- **Customer workspace data (leads, conversations, buyers, files):** for as long as the customer's contract runs. On termination we delete or return it within **30 days**, unless the customer asks us to do so sooner or the law requires us to keep it longer.
- **Technical and security logs:** normally up to 12 months.
- **Contract, invoicing and accounting records:** for the period required by Georgian accounting and tax legislation.

Backups are cycled on a rolling basis; data deleted from the live system may persist in backups for a short period before being overwritten.

## 10. Data security

---

Security measures in place include:

- **Strict tenant isolation.** Every request carries the organisation it belongs to, and access is checked against it on the server. One customer cannot read another's data.
- **Role-based access control.** Administrator, sales lead, agent and marketing roles carry different permissions, enforced on the server rather than merely hidden in the interface.
- **No direct database access from the browser.** The browser talks only to our own API on the same origin; it holds no database key and cannot query storage directly. Uploads and downloads use one-time signed links that expire.
- **Session hardening.** The refresh token is an HttpOnly cookie scoped to the authentication path; the access token lives only in memory.
- **Encryption in transit** for all connections, and encryption at rest by our infrastructure providers.
- **Passwords** are never stored by us in readable form.

No system is perfectly secure, and we do not claim otherwise. If a breach occurs that is likely to cause harm, we will notify the Personal Data Protection Service of Georgia and affected controllers and individuals as the law requires, without undue delay.

## 11. Rights of the data subject

---

Subject to the conditions in applicable law, you may:

- **access** the personal data we hold about you, and ask how it is processed;
- **rectify** data that is inaccurate or incomplete;
- **erase** data, where there is no lawful ground to keep it;
- **restrict** processing while a dispute is resolved;
- **object** to processing based on legitimate interests;
- **receive a copy** of data you provided, in a structured, machine-readable form, and ask for it to be transmitted to another provider where technically feasible;
- **withdraw consent** at any time, where processing rests on consent, without affecting what was done before;

- **not be subject** to a decision based solely on automated processing that produces legal effects. We do not carry out such automated decision-making, and the platform performs no automated profiling or scoring of buyers on our behalf.

To exercise a right, write to [privacy@development360.ge](mailto:privacy@development360.ge). We will respond within the period required by applicable law and, in any event, without undue delay. We may need to verify your identity before acting, and where the data belongs to a customer's workspace we will refer you to that customer as described in section 2.

You may also lodge a complaint with the **Personal Data Protection Service of Georgia** ([personaldata.ge](http://personaldata.ge)). If the GDPR applies to you, you may complain to the supervisory authority where you live or work.

## 12. Children's personal data

---

The platform is a business tool and is not directed at children. We do not knowingly collect data from anyone under 16. Customers must not use the platform to record data about children without a lawful basis. If you believe a child's data has been entered into the platform, tell us and we will refer the matter to the relevant customer for deletion.

## 13. Amendments to this Policy

---

We may update this policy as the platform changes or the law does. The "last updated" date at the top always reflects the current version. Where a change materially affects your rights we will give notice in the application or by email before it takes effect. Continuing to use the platform after a change takes effect means the updated policy applies.

## 14. Contact details

---

შპს დეველოპმენტ 360 (LLC Development 360)

Identification code: 405871310

Tbilisi, Georgia

[privacy@development360.ge](mailto:privacy@development360.ge)

Data subjects whose personal data is held in a customer's workspace should first refer to Section 2. In most cases the customer company, as controller, is responsible for responding to the request.