Gorilla Group Courier Privacy Notice

Applicable in the Republic of Lithuania
Data controller: MB Gorilla Group
Legal entity code: 308088126
Registered office: Partizanų g. 61-806, LT-49282 Kaunas, Lithuania
Version: 9 August 2026

MB Gorilla Group respects courier privacy and protects personal data processed through the Gorilla Group platform, courier application, website and support channels.

This Privacy Notice is intended for Lithuania and applies to the services provided by MB Gorilla Group in the Republic of Lithuania.

Contents

1. About this Privacy Notice
2. Data controller and contacts
3. Personal data we process
4. Purposes and legal bases for processing
5. Recipients of personal data
6. Transfers outside the EEA
7. How we protect personal data
8. How long we retain personal data
9. Courier rights
10. Direct marketing
11. Changes to this Notice

1. About this Privacy Notice

This Privacy Notice (the **Notice**) explains how MB Gorilla Group (**Gorilla Group**, **we**, **us**, **our**) collects, uses, stores and discloses the personal data of individuals who register for or provide delivery services through the Gorilla Group platform (**Couriers**).

This Notice applies to:

- individuals who submit an application to become a Courier;
- self-employed Couriers and delivery service providers lawfully engaged by legal entities;
- individuals who use the Gorilla Group courier application, website, support channels or other delivery-related channels.

Only persons aged 18 or over may register as Couriers. We do not knowingly collect data relating to underage Couriers.

This Notice should be read together with the Gorilla Group Courier General Terms, permission explanations displayed in the application and any additional privacy notices relating to a specific feature.

We process personal data in accordance with Regulation (EU) 2016/679 (the General Data Protection Regulation, the **GDPR**), the Law on Legal Protection of Personal Data of the Republic of Lithuania, the Law on Electronic Communications of the Republic of Lithuania and other applicable Lithuanian and European Union laws.

2. Data controller and contacts

The controller of Courier personal data is:

MB Gorilla Group
Legal entity code 308088126
Partizanų g. 61-806, LT-49282 Kaunas, Lithuania

You may submit privacy questions, data subject requests and complaints:

- through the support or privacy section of the Gorilla Group application;
- through the electronic contact published in the application or on the Gorilla Group website;
- by post to the registered office stated above.

To protect your data, we may reasonably ask you to verify your identity before acting on a request.

3. Personal data we process

We process only the data necessary to register Couriers, arrange delivery services, make payments, maintain safety, comply with law and operate the platform.

The specific data processed depends on the application features used, the selected means of delivery and applicable legal requirements.

3.1. Data you provide

Data category	Examples
Profile and contact data	Name, surname, date of birth, telephone number, email address, place of residence, city, profile picture, language, communication preferences and notification settings.
Account data	Login details, account creation date, status, consents, acceptance of terms, password reset requests and records of account changes. Passwords are protected by technical measures and are not stored as plain text.
Identity and right-to-work data	Identity document details or a copy, personal identification number, citizenship, data confirming the right to reside or work, individual activity certificate or legal entity details, tax identifiers and VAT number where applicable.
Vehicle data	Vehicle type, make, model, registration number, ownership or right of use, driving licence, insurance and roadworthiness inspection data where relevant to the selected delivery vehicle.
Payment and tax data	Bank account and IBAN, payout details, delivery earnings, bonuses, tips, cash balance, deductions, invoices, payment and settlement history, and tax data required by law.
Communications and support data	The content of requests, chats, emails, complaints and incident reports, attached documents, photographs or other files, and the date and time of communications. Telephone calls are recorded only after prior notice and where there is an appropriate legal basis.
Survey and feedback data	Responses to surveys or interviews and feedback about the application, delivery process and quality of support.

3.2. Data generated or collected when you use the platform

Data category	Examples
Location data	Precise or approximate Courier location, timestamps, route, pickup and delivery locations. Location is collected in accordance with device permissions when the Courier is online to receive orders, is completing an active delivery or when location is necessary for a specific application feature. If background access is permitted, location may be collected while the application is running in the background.
Order and delivery data	Order number, Partner, pickup and delivery addresses, date, time, status, estimated and actual delivery time, distance, route, order value, payment method, and accepted, rejected, cancelled and completed orders.
Performance and quality data	Online status, order acceptance and cancellation data, delivery duration, client and Partner feedback, complaints, breaches, warnings, temporary restrictions and account termination information.
Settlement and earnings data	Courier balance, cash received, cash paid to a Partner, earnings, bonuses, tips, corrections, debts, weekly statements and payouts.
Device and technical data	IP address, device and operating system type, application version, language, unique technical identifiers, login sessions, error logs, security events and information about application performance and interaction.
Cookies, SDK and analytics data	Data collected by cookies, software development kits and analytics tools when the website or relevant application features are used. Non-essential analytics and advertising technologies are used only with consent where required by law.

3.3. Data from other sources

We may receive data from:

- restaurants, shops and other platform Partners when they provide information about an order, incident or quality of a Courier's service;
- Clients who submit ratings, complaints, safety reports or delivery information;
- identity, payment, maps, communications, fraud prevention and other service providers where we use those services;
- public registers, the tax authority, law enforcement or other public authorities where permitted or required by law;
- publicly available sources where necessary for a specific and lawful verification.

3.4. Special-category and biometric data

We do not normally collect data concerning health, political opinions, religious beliefs or other special categories of personal data. Please do not provide such data unless it is necessary to investigate a specific incident or meet a legal obligation.

This Notice does not provide for biometric facial recognition. If biometric identity verification is introduced in the future, Couriers will receive separate and clear information in advance and, where required, explicit consent will be obtained or another lawful basis will be established.

4. Purposes and legal bases for processing

Under the GDPR, we process personal data on one or more of the following legal bases:

- **steps before entering into and performance of a contract**, where data is necessary for registration, platform services, order fulfilment or settlement;
- **compliance with a legal obligation**, where data must be processed under tax, accounting, anti-money laundering, law enforcement or other laws;
- **legitimate interests**, where processing is necessary for safety, fraud prevention, service quality, dispute resolution, system security or business administration and the Courier's rights do not override those interests;
- **consent**, where we ask for it for optional analytics, marketing, a specific device function or another clearly stated purpose.

Processing purpose	Main data used	Legal basis
Receive and assess an application, create and administer an account	Profile, account, identity, activity and vehicle data	Steps before entering into a contract, performance of a contract, legal obligation, legitimate interests
Verify the Courier's identity, age, right to work and vehicle compliance	Identity, activity, vehicle, device and security data	Performance of a contract, legal obligation, legitimate interests
Offer, allocate and facilitate delivery orders	Location, order, online-status, performance, device and communication data	Performance of a contract, legitimate interests
Show delivery progress to the Client and Partner and enable communication	Courier's first name, order status, location during an active delivery and in-app contact details	Performance of a contract, legitimate interests
Calculate Courier remuneration and administer cash, payouts, invoices and taxes	Order, location, earnings, bank, payment and tax data	Performance of a contract, legal obligation
Provide support and investigate complaints, incidents and disputes	Account, order, location, communication, payment, feedback and uploaded file data	Performance of a contract, legitimate interests, legal obligation
Protect the platform, Clients, Partners and Couriers and detect fraud or misuse	Identity, device, location, order, payment, performance and communication data	Legitimate interests, legal obligation
Maintain and improve the application, correct errors and perform analysis	Device, technical, usage, order, location and de-identified statistical data	Legitimate interests; consent for non-essential analytics technologies
Send service-related communications	Name, telephone number, email address, account and order data	Performance of a contract, legal obligation
Send marketing communications and assess their effectiveness	Contact data, communication choices, application usage and consent records	Consent or an exception expressly permitted by law
Meet accounting, tax and reporting obligations, including statutory platform-operator reporting	Profile, tax, payment, earnings and order data	Legal obligation
Establish, exercise or defend legal claims and respond to lawful authority requests	Data necessary in view of the particular claim or request	Legal obligation, legitimate interests

Where processing is based on consent, you may withdraw that consent at any time. Withdrawal does not affect the lawfulness of processing carried out before withdrawal.

4.1. Use of location data

Location data is necessary to:

- offer nearby orders;
- calculate distance, estimated delivery time and remuneration;
- support route selection;
- show the progress of an active order to the Client and Partner;
- investigate delivery, safety, fraud or settlement incidents.

The Courier can control location permissions in the device settings. If necessary location access is disabled, some or all courier application functions may not work. When the Courier is not online to receive orders and is not completing an active delivery, location data should not be collected except where necessary for security, error diagnostics or a function expressly enabled by the Courier.

4.2. Automated assessment and decisions

We may use rules or automated tools to flag suspicious activity, technical errors, possible fraud or breaches of the Terms. An automated alert alone will not be the final basis for terminating a Courier account or making another decision that has legal or similarly significant effects. Before such a decision, the data and circumstances are reviewed by an authorised employee, and the Courier is given an opportunity to provide an explanation and challenge the decision.

5. Recipients of personal data

We disclose personal data only to the extent necessary for a specific purpose.

Recipient category	Circumstances and data that may be disclosed
Clients	During an active order, the Client may see the Courier's first name, delivery status, approximate or precise location and an in-app contact method. Location is no longer displayed after completion or cancellation, without prejudice to lawfully retained delivery history.
Restaurants, shops and other Partners	A Partner may see the Courier's first name, order number, arrival and pickup status and contact method to the extent necessary to hand over an order and resolve an incident.
Payment and financial service providers	Banks, payment intermediaries, accounting and tax service providers receive only the data necessary for payments, payouts, invoicing and legal compliance.
IT and infrastructure service providers	Providers of hosting, storage, authentication, communications, customer support, error monitoring, maps, routing and analytics may process data on our behalf under contracts and instructions.
Identity and compliance verification providers	Where such providers are used, they receive only the data necessary to verify identity, document validity or the right to conduct the activity.
Insurers, legal advisers and debt administration providers	Data may be disclosed when handling an insurance event, incident, debt, dispute or legal claim.
State and municipal authorities	The State Tax Inspectorate, State Social Insurance Fund Board, police, courts, the State Data Protection Inspectorate and other authorities may receive data where disclosure is required by law or a valid binding request.
Business successors	In the event of a reorganisation, merger or sale of the business or part of it, data may be transferred to a lawful successor subject to confidentiality and notice where required by law.

We select service providers after assessing their security and privacy controls. Processors may use personal data only in accordance with our documented instructions, contract and applicable law.

We do not sell Courier personal data.

6. Transfers outside the EEA

The Gorilla Group platform is intended for the Lithuanian market. However, some of our IT, communications, maps, analytics or other service providers may process data in or outside the European Economic Area (EEA).

Where personal data is transferred outside the EEA, we ensure protection under Chapter V of the GDPR. Depending on the recipient and country, we rely on:

- a European Commission adequacy decision;
- the European Commission's Standard Contractual Clauses and, where necessary, additional technical and organisational safeguards;
- another transfer mechanism or derogation permitted by the GDPR.

Information about the safeguards applicable to a specific transfer may be requested through the channels listed in Section 2.

7. How we protect personal data

We use technical and organisational measures appropriate to the risk, including:

- encryption in transit and, where appropriate, encryption at rest;
- access restrictions based on staff duties;
- account authentication and monitoring of sessions and security events;
- backups, system updates, vulnerability management and incident procedures;
- confidentiality obligations for staff and service providers;
- data minimisation, retention schedules and secure data destruction.

The Courier is also responsible for keeping login credentials confidential, maintaining a secure device and not allowing another person to use the account.

No system is completely secure. If a personal data breach is identified, we take steps to contain it and, where required, notify the State Data Protection Inspectorate and affected individuals.

8. How long we retain personal data

We retain data no longer than necessary for the purpose for which it was collected or for the period required by law. A period may be extended where there is a dispute, investigation or audit or where data must be retained for a legal claim.

Data category	Usual period or retention criterion
Incomplete or rejected application data	Up to 6 months after withdrawal or a final decision, unless the data is needed for a complaint, investigation or legal obligation.
Account and profile data	While the account is active and for up to 3 years after closure, except where data must be retained for longer.
Identity and activity documents	While necessary to verify identity and lawful activity; after account closure, only for as long as necessary for a legal obligation, fraud prevention or legal claims.
Order, route and location data	Normally up to 2 years after delivery, unless a shorter period is sufficient or a longer period is required for a dispute, safety incident, accounting or legal obligation.
Payment, invoice, earnings and tax data	For the period required under Lithuanian law; accounting and tax documents are generally retained for 10 years.
Support requests, chats, complaints and incidents	Normally up to 3 years after closure of the request; longer where an investigation or dispute is ongoing or law requires it.
Technical and security logs	Normally up to 2 years, depending on purpose, risk and the need to investigate incidents.
Marketing choices	Until consent is withdrawn or an opt-out is submitted. Evidence of consent and opt-out may be retained for a further 3 years to demonstrate compliance.

When the retention period expires, data is deleted, securely destroyed or irreversibly anonymised. Anonymised statistical information from which a person can no longer be identified may be used for longer.

Deleting the application from a device does not delete the account or its data. An account may be closed through the application, where that function is available, or by submitting a request under Section 2.

9. Courier rights

In the circumstances set out in the GDPR, you have the right to:

- **access** your personal data and receive a copy;
- **rectify** inaccurate or incomplete data;
- **request erasure** where there is no lawful ground to retain the data;
- **restrict processing** in the circumstances set out in the GDPR;
- **object** to processing based on legitimate interests, including an absolute right to object to direct marketing;
- **receive and transmit data** that you provided and that is processed automatically on the basis of consent or contract;
- **withdraw consent** at any time;
- **request human intervention**, express your view and challenge a decision if you are subject to a solely automated decision producing legal or similarly significant effects;
- **lodge a complaint** with a supervisory authority or bring court proceedings.

A request may be submitted through the channels listed in Section 2. We normally respond within one month after receipt. For a complex request or several requests, the period may be extended by two further months, in which case we will notify you and explain the reason.

Rights are not absolute. For example, we cannot erase data that must be retained under accounting or tax law or that is necessary to establish or defend a legal claim.

In Lithuania, you may lodge a complaint with:

State Data Protection Inspectorate (VDAI)
L. Sapiegos g. 17, LT-10312 Vilnius, Lithuania
Website: https://vdai.lrv.lt/

We invite you to contact us first so that we can address your concern, but this does not restrict your right to complain directly to the supervisory authority.

10. Direct marketing

We send marketing communications by email, SMS, push notification or other electronic communication channel only:

- with the Courier's consent; or
- where the existing-relationship and similar-services exception under the Law on Electronic Communications of the Republic of Lithuania applies, with a clear, free and easy means to opt out.

You may opt out at any time by using the unsubscribe link, changing notification settings in the application or contacting us through the channels listed in Section 2.

Service communications concerning an account, order, payout, security, changes to terms or application operation are not direct marketing. They may be necessary to perform a contract or comply with a legal obligation.

11. Changes to this Notice

We may update this Notice when platform features, data processing or applicable law change. The latest version is published in the Gorilla Group application or on the website and states the date of the update.

Where required by law, we will notify Couriers in advance of material changes that significantly affect their rights or how their data is used, through the application, email or another appropriate channel.

Official references:

- General Data Protection Regulation (EU) 2016/679
- State Data Protection Inspectorate of Lithuania
- Law on Electronic Communications of the Republic of Lithuania
- European Commission information on international data transfers