Privacy Policy – Mopka Platform

Last updated: 24.11.2026 · Download PDF

This Privacy Policy (hereinafter: "Policy") contains information about the processing of your personal data in connection with the use of the "Mopka" platform, operating at https://mopka.pl, https://mopka.cz and https://app.mopka.pl (hereinafter: "Platform"). Capitalized terms not otherwise defined in this Policy have the meanings given to them in the Terms of Service available at https://mopka.pl/regulamin.

Data Controller

The controller of your personal data is Daniel Kołban operating under the business name Daniel Kołban "Dan-Kol", address: Chechlana 7A, 32-593 Żarki, Poland, NIP (Tax ID): 6783224870, REGON: 540993796 (hereinafter: "Controller").

Contact the Controller

For all matters related to personal data processing, you may contact the Controller via email at: kontakt@mopka.pl.

Data Protection Measures

The Controller applies modern organizational and technical safeguards to ensure the best possible protection of your personal data. The Controller guarantees that data is processed in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR), the Polish Act of 10 May 2018 on the protection of personal data, and other applicable data protection regulations.

Information About Processed Personal Data

Using the Platform requires the processing of your personal data. Below you will find detailed information about the purposes and legal bases for processing, retention periods, and whether providing data is mandatory or voluntary.

Purpose of processing	Conclusion and performance of the Service Agreement
Processed data	First and last name, company name, type of business, email address, phone number, NIP (Tax ID), password

	(encrypted)
Legal basis	Art. 6(1)(b) GDPR (processing necessary for the performance of a contract) and Art. 6(1)(f) GDPR (legitimate interest of the Controller – enabling access to the Platform)
Voluntary nature	Providing data is voluntary but necessary for the conclusion and performance of the Agreement (including creating an Account).
Retention period	Until the expiry of limitation periods for claims arising from the Agreement.

Purpose of processing	Finding out how you reached the Platform and counting sign-ups from ads
Processed data	The ad or campaign tag from the page address (the Google ad click ID "gclid" and "utm" parameters), the address of the page you came from and the first page you visited, saved when you register an Account
Legal basis	Art. 6(1)(f) GDPR (legitimate interest of the Controller – assessing the effectiveness of its own ads)
Voluntary nature	The data is saved automatically when the page address contains an ad or campaign tag. If you sign up during a later visit, the tag is available only if you have consented to marketing cookies.
Retention period	Until the Account is deleted or an objection is successfully raised.

Purpose of processing	Sending SMS and email notifications
Processed data	Email address, phone number
Legal basis	Art. 6(1)(f) GDPR (legitimate interest of the Controller – informing about activities related to the performance of the Agreement)

Voluntary nature	Providing data is voluntary but necessary for receiving system notifications.
Retention period	Until a successful objection is raised or the purpose of processing is achieved.

Purpose of processing	Direct marketing of the Controller's own services (information about new Platform features and offers, sent by email or SMS)
Processed data	Email address, phone number, first name
Legal basis	Art. 6(1)(a) GDPR (consent) in connection with Art. 398 of the Polish Electronic Communications Law of 12 July 2024. Consent is given separately for each channel (email, SMS), at Account registration or in the Account settings.
Voluntary nature	Giving consent is voluntary and its absence does not affect the use of the Platform. Consent can be withdrawn at any time in the Account settings; withdrawal does not affect the lawfulness of processing carried out before it.
Retention period	Until consent is withdrawn. Proof of consent and of its withdrawal (wording, date, IP address) is kept by the Controller until claims become time-barred.

Purpose of processing	Processing complaints
Processed data	First and last name, email address
Legal basis	Art. 6(1)(f) GDPR (legitimate interest of the Controller – pursuing or defending against claims)
Voluntary nature	Providing data is voluntary but necessary for processing the complaint.
Retention period	For the duration of the complaint procedure, and then until the expiry of limitation periods.

Purpose of processing	Fulfilling tax obligations (issuing invoices, storing accounting documentation)
Processed data	First and last name / company name, registered address, NIP (Tax ID)
Legal basis	Art. 6(1)(c) GDPR (fulfilling a legal obligation – obligations under tax law)
Voluntary nature	Providing data is voluntary but necessary for the Controller to fulfill tax obligations.
Retention period	For 5 years from the end of the year in which the tax payment deadline expired.

Purpose of processing	Fulfilling data protection obligations (exercising GDPR rights)
Processed data	First and last name, contact details (email)
Legal basis	Art. 6(1)(c) GDPR (fulfilling a legal obligation – data protection regulations)
Voluntary nature	Providing data is voluntary but necessary for exercising your rights under GDPR.
Retention period	Until the expiry of limitation periods for claims related to data protection violations.

Purpose of processing	Establishing, pursuing, or defending against claims
Processed data	First and last name / company name, email address, NIP (Tax ID)
Legal basis	Art. 6(1)(f) GDPR (legitimate interest of the Controller – establishing, pursuing, or defending against claims)
Voluntary nature	Providing data is voluntary but necessary for the above purposes.
Retention period	Until the expiry of limitation periods for claims.

Purpose of processing	Traffic statistics for the Platform's website
Processed data	IP address, date and time of visits, pages visited, country, browser and operating system type
Legal basis	Art. 6(1)(f) GDPR (legitimate interest of the Controller – aggregate traffic information that helps improve the Platform)
Voluntary nature	The data is collected automatically by Cloudflare, whose servers carry the traffic to the Platform. The statistics do not use cookies, and the Controller sees them only in aggregate form.
Retention period	Until a successful objection is raised or the purpose of processing is achieved.

Purpose of processing	Platform administration (server logs)
Processed data	IP address, request date and time, browser and operating system information
Legal basis	Art. 6(1)(f) GDPR (legitimate interest of the Controller – ensuring proper Platform operation)
Voluntary nature	Data is recorded automatically each time the Platform is used.
Retention period	Until a successful objection is raised or the purpose of processing is achieved.

Purpose of processing	Keeping the Platform secure and preventing abuse (checks of new sign-ups, protection of sign-in)
Processed data	Email address, IP address and the country you connect from, phone number, browser information, history of sign-in attempts
Legal basis	Art. 6(1)(f) GDPR (legitimate interest of the Controller – protecting the Platform and its users against abuse)

Voluntary nature	The data is recorded automatically at sign-up and sign-in.
Retention period	History of sign-in attempts – 90 days; sign-up data – until the Account is deleted.

Purpose of processing	Handling user inquiries
Processed data	First name, email address, other data included in the message
Legal basis	Art. 6(1)(f) GDPR (legitimate interest of the Controller – responding to inquiries)
Voluntary nature	Providing data is voluntary but necessary for receiving a response.
Retention period	Until a successful objection is raised or the purpose of processing is achieved.

Recipients of Personal Data

Recipients of personal data may include the following external entities cooperating with the Controller:

1. Stripe Payments Europe Ltd., based in Dublin (Ireland), part of the Stripe, Inc. group – online payment processing (the Controller does not store payment card data);
2. LINK Mobility Poland sp. z o.o., Gliwice, operator of SMSAPI – SMS delivery service provider;
3. Resend, Inc. – email delivery service provider;
4. Cloudflare, Inc., San Francisco (USA) – the server network that carries traffic to the Platform and protects it against attacks (data: IP address, browser information, addresses visited);
5. external invoicing system providers used by the Subscriber (e.g., Fakturownia, iFirma, inFakt) – to the extent necessary for invoice issuance;
6. cyber_Folks S.A., Poznań – the server the Platform runs on, including storage of files uploaded to the Platform (photos, logos, documents), and backups;
7. accounting services provider;
8. Functional Software, Inc. d/b/a Sentry, based in San Francisco (USA) – application error monitoring service used to improve the quality and security of the Platform (scope of data:

user ID, email address, IP address, browser and error information, and, after your consent to analytics cookies in the app, also a recording of the last moments of the session in which the error occurred, with text hidden and no images);

9. Hetzner Online GmbH, Gunzenhausen (Germany) – storage of encrypted backups outside the Platform server (once they are set up);
10. Infakt sp. z o.o., based in Kraków – issuing invoices for the Paid Plans of the Platform;
11. OpenStreetMap Foundation, based in the United Kingdom – the map in the app and locating the addresses you enter (scope of data: IP address, the address entered, browser information);
12. providers of push notification services of browsers and operating systems (e.g. Google, Apple, Mozilla) – delivering notifications to your device if you turn them on (the content of a notification is encrypted, and the provider only sees the identifier of your subscription);
13. KEPTAGO LTD, Paphos (Cyprus), the operator of the Geoapify service – address suggestions while an address is being typed in the Platform (once this feature is turned on; scope of data: the address being typed or a part of it and the approximate area where the Subscriber works, to within about 10 km; the requests are sent by the Platform server, so Geoapify does not receive your IP address or information about your browser).

Additionally, personal data may be transferred to public or private entities if required by applicable law, a final court judgment, or a final administrative decision.

Transfer of Personal Data to Third Countries

In connection with the Controller's use of services by Stripe Payments Europe Ltd. (Ireland, with onward transfer to Stripe, Inc. in the USA), Cloudflare, Inc. (USA), Resend, Inc. (USA), Functional Software, Inc. d/b/a Sentry (USA) and push notification providers (e.g. Google, Apple, Mozilla), your personal data may be transferred to the United States, and in connection with the use of OpenStreetMap Foundation maps, to the United Kingdom. The legal basis for the transfer is the European Commission's implementing decision on the adequacy of data protection provided under the EU-US Data Privacy Framework (for entities certified under it), the European Commission's adequacy decision for the United Kingdom, or standard contractual clauses approved by the European Commission (Art. 46(2)(c) GDPR). Files uploaded to the Platform (photos, logos, documents) are stored on servers located in the European Economic Area. You may obtain from the Controller a copy of the safeguards applied to transfers to a third country.

Your Rights

In connection with the processing of personal data, you have the following rights:

1. Right of access – you have the right to information about what personal data concerning you is processed by the Controller and to receive a copy thereof. The first copy is free; the Controller may charge a fee for subsequent copies.
2. Right to rectification – if processed data becomes outdated or incomplete, you have the right to request its rectification.
3. Right to erasure – in certain situations, you may request the deletion of your personal data, e.g., when the data is no longer needed, you have successfully withdrawn consent, processing is unlawful, or erasure is required by a legal obligation.
4. Right to data portability – if data is processed based on consent or for the performance of a contract, you have the right to transfer your data to another controller (Art. 20 GDPR).
5. Right to withdraw consent – if processing is based on consent, you may withdraw it at any time. Withdrawal does not affect the lawfulness of processing carried out before withdrawal.
6. Right to restriction of processing – if you believe data is inaccurate, processing is unlawful, or the Controller no longer needs certain data, you may request restriction of processing.
7. Right to object – you have the right to object to processing based on the Controller's legitimate interest. If the objection is successful, the Controller will cease processing data for the given purpose.
8. Right to lodge a complaint – you have the right to lodge a complaint with the President of the Personal Data Protection Office (UODO) if you believe that data processing violates GDPR provisions.

Account Deletion and Data Export

1. You have the right to export your data in a portable format (in accordance with Art. 20 GDPR). The export function is available in Settings under "Backups and account".
2. You may request Account deletion in the Platform settings. After submitting the request, a 30-day grace period begins, during which you may reverse your decision.
3. After 30 days, the Account is permanently deleted along with all data, subject to data whose retention is required by law. Data disappears from encrypted backups as they rotate, no later than after 35 days.
4. System logs (AuditLog) may be retained by the Controller even after Account deletion, for 2 years (entries about deletions, refunds and exports for 7 years), based on Art. 6(1)(f) GDPR (legitimate interest – ensuring Platform security and accountability).

Cookies

1. The Platform uses cookies installed on your device. These are small text files that can be read by the Controller's system.
2. The Controller uses cookies for the following purposes:
   - ensuring proper Platform operation – cookies enable smooth use of Platform features;
   - measuring ad effectiveness – with your consent to marketing cookies, we remember which ad or campaign brought you to the site, so we can count sign-ups from ads;
   - improving user comfort – cookies enable error detection and adapting the Platform to user preferences.
3. The Controller may place persistent and temporary (session) cookies. Session cookies are deleted when you close your browser.
4. Cookie information is displayed in a banner at the bottom of the Platform's website. You can enable or disable cookies for individual categories (except necessary ones) and change these settings at any time.
5. The cookies needed for signing in link the browser to your Account; other cookies are not used to identify you.

Tool	Provider	Functions and data scope	Duration
Necessary cookies	Mopka (Controller)	Necessary for the Platform to work properly (among others: keeping you signed in, remembering the device for two-step sign-in, recording your cookie choice, the language and settings kept in browser storage). They cannot be disabled.	Session, up to 30 days (sign-in) and up to 12 months (record of consent)
Visit source	Mopka (Controller)	Remembers which ad or campaign brought you to the site (gclid, utm) until you register an Account. Saved only with your consent to marketing cookies.	90 days

Through your browser, you can check whether cookies have been installed on your device, delete them, and block their future installation. However, disabling cookies may cause difficulties in using the Platform.

Final Provisions

In matters not regulated by this Policy, generally applicable data protection regulations shall apply. This version of the Policy is effective from 24 November 2026. Privacy Policy as worded

on 29 October 2026 (PDF)

← Back to homepage