MapCaller Privacy Policy

English

Version: 2026-09-13-v1

Effective date: 13 September 2026

Data Controller: K&H Digital Sp. z o.o., ul. Podmiejska 20, 01-498 Warszawa, Poland | KRS 0001005137 | NIP 5423459599 | REGON 523790365

Privacy contact: privacy@kihedi.com

Product: MapCaller is an independent product and is not affiliated with, sponsored by or endorsed by Google.

1. Scope

This Privacy Policy explains how personal data is processed when a person uses the MapCaller website, browser extension, cloud service, account, payments, support and related features.

It applies to website visitors; people creating an account or signing in with Google; Owners, Admins, Supervisors and Operators within customer organizations; payers and customer contacts; people contacting support; and, in a limited scope, individuals whose professional or contact data a customer stores in a MapCaller workspace.

2. GDPR roles

K&H Digital acts as an independent controller for account registration, Google OAuth and user identification, organization/role/invitation/device management, subscriptions, payments, invoicing and tax records, security and abuse prevention, support and claims, and mandatory service/legal communications.

For business/contact data placed in a workspace, the customer organization normally determines what data to store and how to use it and therefore acts as controller, while K&H Digital processes such data on the customer's behalf to provide the service. A Data Processing Agreement may apply where required. K&H Digital does not determine the legal basis for cold calls, messages, direct marketing or adding a particular contact; that remains the customer's responsibility.

3. Data we process

Account and identification data may include Google account identifier/subject, name or display name, e-mail address, e-mail verification information where available, organization ID, user ID and role, operator number, language/locale/time zone, account status and creation/activation/deactivation dates.

Organization and subscription data may include organization/workspace name, Owner/admin details, plan, seat quantity, licence/subscription status and periods, billing name/address, VAT ID/NIP or other tax number, payment-provider customer/subscription/payment identifiers, invoices, payment status and billing history. K&H Digital does not store full card numbers; card data is handled by the payment provider.

Device and security data may include device ID, registration identifier, device name, operating system/browser, registration and last-activity dates, active/revoked status, extension version and API compatibility, token/session/security identifiers and credential hashes, IP address, user agent, timestamps and technical metadata necessary for security, rate limiting, proof of legal acceptance and abuse prevention, together with safe diagnostic/error context that should not contain secrets.

Workspace company/contact data may include external identifiers such as Google Place ID, company name, address, website, coordinates, Google Maps URL, telephone numbers in source and normalized form, and first/last-seen dates. This may be non-personal company data, but becomes personal data where it identifies an individual, sole trader or company representative.

Contact-history data may include organization, company and acting user, channel (phone, WhatsApp or phone_then_whatsapp), result/status code, user comment, device/server time and time zone, event UUID,

correction/cancellation information, operator name/number and authorship. Users must not place special-category, health, political, religious, intimate-life, criminal-conviction, identity-document, payment-card or other excessive confidential information in comments.

Temporary presence/collaboration data may include user ID, company ID, session token and presence start/expiry time. Presence should not be stored as permanent contact history.

If Google Sheets integration is enabled, MapCaller may process spreadsheet ID/name, configuring user, export status/time, technical error codes and selected contact-session data.

Support data may include e-mail/contact details, request content, user-provided attachments/screenshots, technical information needed for diagnosis, and response/resolution history.

4. Sources of data

Data may come directly from the user, from an organization administrator inviting the user, from Google through OAuth within the scope shown to the user, from user actions in the extension/service, from a public Google Maps business card opened and processed by the user, from the payment provider, from technical/security logs, and from a Google Sheet connected by the user.

K&H Digital does not claim to independently verify the accuracy of Google Maps or other external-source data.

5. Purposes and legal bases

Contract / pre-contract steps - Article 6(1)(b) GDPR: account creation and login; provision of MapCaller functions; organization, role, licence and device management; contract-related support; and payment/subscription processing to the extent necessary for contract performance.

Legal obligation - Article 6(1)(c) GDPR: accounting, tax and invoicing; compliance with court, authority or statutory requirements; and mandatory consumer/documentation obligations.

Legitimate interests - Article 6(1)(f) GDPR: account/infrastructure security; fraud, abuse, licence-circumvention and unauthorized-access prevention; prevention of repeated use of the one-time voluntary 14-day first-payment refund through the same MapCaller account / same Google account identifier after refund, re-registration or creation of a new organization; rate limiting, audit and incident investigation; establishment, exercise or defence of legal claims; and necessary operational analytics/reliability improvements, preferably on aggregated or de-identified data. Legitimate interests are not relied upon where an individual's interests or fundamental rights override them.

Consent - Article 6(1)(a) GDPR: only where separately requested, for example optional marketing communications, optional analytics/advertising cookies or other functions not necessary for the contract. Consent may be withdrawn without affecting prior lawful processing.

For contact/CRM data processed on the customer's instructions, the customer determines the legal basis as controller and K&H Digital acts on documented instructions and the data-processing agreement.

6. Customer obligations for contact data

The customer must have a lawful basis for storing and using data; comply with direct-marketing, calling and messaging rules; provide Articles 13/14 GDPR information where required; respect objections, opt-outs and do-not-contact requests; limit employee access by role; avoid excessive or prohibited data; and correct or delete data when required by law.

MapCaller is a work tool and does not itself create a legal basis for a call or message.

7. Recipients

Data may be disclosed, only to the extent necessary, to cloud/database infrastructure providers; Google OAuth and related Google-function providers; payment and invoice providers; e-mail, monitoring, security and technical-support providers; Google Sheets when the customer enables export; accountants, lawyers and professional advisers; public authorities and courts where required by law; and a business acquirer in a lawful reorganization subject to data-protection requirements.

A more specific list of technical providers may be maintained separately and made available to business customers or published as a Subprocessor List.

8. Google Maps, WhatsApp and external platforms

When using Google Maps, a Google account, WhatsApp or other platforms, the user also interacts with those operators under their own terms and privacy policies.

Opening a telephone call or WhatsApp chat is normally initiated directly by the user in the browser or operating system. K&H Digital does not control subsequent processing by the telecom operator, Google, Meta or WhatsApp.

9. International transfers

Some providers may process data outside Poland or the European Economic Area. Where GDPR requires safeguards, applicable mechanisms may include an European Commission adequacy decision, Standard Contractual Clauses, supplementary technical/organizational measures, or another lawful transfer mechanism.

Actual hosting regions, provider roles and transfer safeguards should be maintained and reviewed as the production provider set evolves.

10. Retention

Account and organization data is retained for the active contract and afterwards for as long as reasonably necessary for account closure, security and legal claims.

Customer workspace data and contact history are retained during the subscription and for 30 days after it ends to allow available export, after which they are deleted or irreversibly anonymized except where a lawful exception applies. Presence data is short-lived until technical-session expiry. Invitations are retained until accepted, expired or revoked and then for a limited period for security/audit. Revoked-device history is retained as needed for security history and prevention of repeated unauthorized access.

Billing, invoice and tax records are retained for the periods required under Polish law and accounting rules. Support records are retained until closure and then as necessary for claim protection. Security, audit, diagnostics and backups are retained according to risk-proportionate schedules. Data is not kept indefinitely merely because technically possible.

11. Account deletion and subscription end

After cancellation, the user loses the right to continued paid use, while the organization receives the contractual 30-day export window where the corresponding export function is available.

After that window, data is deleted or anonymized except for accounting/tax records, minimal security/audit records, data needed for an ongoing dispute/fraud investigation/legal obligation, and backups until scheduled secure rotation.

12. Individual rights

Depending on the situation, an individual may have the right to information, access, rectification, erasure, restriction, objection to processing based on legitimate interests, data portability where applicable, withdrawal of consent, and complaint to a supervisory authority.

Where K&H Digital acts as processor for a customer, a request may be directed to that customer as controller and K&H Digital will provide reasonable assistance. Additional information may be requested to verify identity and prevent disclosure of another person’s data.

13. Supervisory complaint

A complaint may in particular be submitted to the President of the Personal Data Protection Office (Prezes Urzędu Ochrony Danych Osobowych - UODO), Poland. This does not limit the right to seek judicial protection.

14. Automated decisions

MapCaller does not make decisions producing legal or similarly significant effects for the user solely by automated means.

Automated security controls may temporarily block login, a third device, an obsolete client version, a suspicious request or rate-limit excess. Such measures protect the service and can be reviewed through support.

15. Security

Risk-appropriate measures include organization-scoped access, server-side authorization and entitlement, role-based access restrictions, up to two registered devices and revocation, limited-life tokens and revocation mechanisms, minimum client version controls, rate limiting and replay/idempotency controls, safe-context audit/diagnostics, restricted production packages without secrets in the extension, and backup/monitoring/incident-response measures as the product evolves.

No internet service can guarantee absolute security.

16. Children

The service is intended for professional and commercial use and is not intended for persons under 18. K&H Digital does not knowingly collect children’s data for the purpose of providing MapCaller.

17. Changes to this Policy

This Policy may be changed when the product, law, providers or processing methods change. Material changes may be communicated through the account, e-mail or website. The policy date and version are maintained.

18. Contact

For privacy questions, exercise of rights and complaints: K&H Digital Sp. z o.o., ul. Podmiejska 20, 01-498 Warszawa, Poland; e-mail: privacy@kihedi.com.