Information Notice for the eMotion Mobile Application

1. Who is responsible for processing your personal data?

This Privacy Notice explains how we collect, use, share and otherwise process personal data when you use the OMV eMotion Mobile Application and related services (the "Application" or "eMotion Application/eMotion App").
We process your personal data in accordance with the General Data Protection Regulation (EU) 2016/679 ("GDPR").
By registering, you confirm that you have read this Notice. Defined terms have the meaning given in the Application Terms and Conditions.
Private Customers may also access the OMV Benefits Program (the "Benefits Program"), shared with OMV MyStation. Both applications access one loyalty account and profile, although the eMotion charging account may remain separate.
Depending on the country where the eMotion App services are provided, the following entities may act as controllers:

- **Austria**: OMV Downstream GmbH, Trabrennstraße 6-8, A-1020 Vienna, Austria, and OMV International Services GmbH, Trabrennstraße 6-8, A-1020 Vienna. More in detail:

    - OMV International Services GmbH acts as controller for the operation of the eMotion app and account management.
    - OMV Downstream GmbH acts as controller for local marketing activities and the Benefits Program.
    - OMV International Services GmbH and OMV Downstream GmbH act as joint controllers for the provision of charging services in Austria.

- **Slovakia**: OMV Slovensko, s.r.o., Einsteinova 25, 851 01 Bratislava, registered in the Commercial Register of the Municipal Court Bratislava III, Section: Sro, Insert No.: 777/B, and OMV International Services GmbH, Trabrennstraße 6-8, A-1020 Vienna. More in detail:
    - OMV International Services GmbH acts as controller for the operation of the eMotion app and account management.
    - OMV Slovensko, s.r.o. acts as controller for local marketing activities and the Benefits Program.
    - OMV International Services GmbH and OMV Slovensko, s.r.o. act as joint controllers for the provision of charging services in Slovakia.

- **Romania:** OMV Petrom Marketing SRL (22 Coralilor Street, Infinity Building, 1st Floor, Oval B, Sector 1, Bucharest; Trade Register J40/10637/1998; registration code 11201891, RO) and OMV International Services GmbH are joint controllers for charging in Romania. OMV Petrom Marketing SRL processes Romanian customer data when charging takes place in Romania. OMV Petrom Marketing SRL is controller for Romanian eMotion users participating in the Benefits Program.

- **Hungary**: OMV Hungária Kft., Október huszonharmadika utca 6-10 5th flr. 5/A., HU-1117 Budapest, and OMV International Services GmbH, Trabrennstraße 6-8, A-1020 Vienna. More in detail:

- OMV International Services GmbH acts as controller for the operation of the eMotion app and account management.
- OMV Hungária Kft. acts as controller for local marketing activities and the Benefits Program.
- OMV International Services GmbH and OMV Hungária Kft. act as joint controllers for the provision of charging services in Hungary.

and

- **OMV International Services GmbH,** Trabrennstraße 6-8, A-1020 Vienna is controller for processing through the eMotion App. Each relevant entity is referred to as the "Controller".

Country-specific provisions appear in **Section 8** below.

2. Categories of Data Subjects

This Privacy Notice applies differently depending on how you access and use the Application:

2.1. Business Users

Business Users access charging services through a business partner, which may provide their activation details. Business Users may manage accounts, stations and sessions; we process their data to provide the service, prevent fraud, comply with law and send functional messages needed to activate or administer those.
Marketing, location-based marketing profiling and Benefits Program participation do not apply to Business Users.

2.2. Private Customers

Private Customers register for private use. They may consent to marketing, location-based marketing profiling and non-essential analytics. Refusal or withdrawal affects only that optional processing, not the account or access to charging services.

2.3. Loyalty Participants

Loyalty Participants are Private Customers who join the Benefits Program.
Participation is optional and governed by the program terms. Participants may receive general or personalized discounts, coupons, rewards and offers.
When you apply for the Benefits Program through the eMotion App, we use your email to verify whether an existing loyalty account is already associated with you, securely link your account where applicable, prevent duplicate registrations and manage your participation in the program. If no account exists, we send the necessary registration data to the common loyalty backend.
The eMotion and OMV MyStation accounts remain distinct. Unless stated otherwise, marketing settings are also kept separate. Disconnecting or deleting your eMotion account does not determine the deletion of your OMV MyStation account or its data.
The data processing described above is necessary to take pre-contractual measures and perform the Benefits Program Contract.

3. What Personal Data do we process and why?

Purpose of Processing	Data Subjects' Categories	Data Categories	Legal Basis
Registration and Account Management	• Business Users • Private Customers	• IP address, type of operating system, type of device used	• Art. 6(1)(b) GDPR – Performance of a contract between the parties

(granting access to the Application in accordance with its General Terms and Conditions)	• Loyalty Participants	• name, address, email address, gender, date of birth and other account information, as applicable. For Business Users, we may receive the email address and other necessary activation information from the referring business partner. • Apple ID or Google profile if the Account is created by the use of these. In such a case, the Participant's personal data will be transferred and will be subject to the privacy policy of Apple (Legal - Apple Privacy Policy - Apple) or of Google LLC (see Privacy Policy - Privacy & Terms - Google), please consult their privacy policies.	(represented by the General Terms and Conditions of the App) Article 6(1)(f) GDPR – legitimate interests in administering the business charging arrangement, as applicable.
Payments and invoicing	• Private Customers • Loyalty Participants	Payment method, transaction data, invoice data	• Art. 6(1)(b) GDPR - Performance of a contract; • Art. 6(1)(c) GDPR - Legal obligation
Charging session management and fraud prevention	• Business Users • Private Customers • Loyalty Participants	Charging logs, identification-medium identifier, charging-station location and usage information, account and transaction data	• Art. 6(1)(b) GDPR – Performance of a contract; • Art. 6(1)(f) GDPR – Legitimate interests in managing and controlling charging processes and preventing fraud
Application Administration, including complaints and queries handling	• Business Users • Private Customers • Loyalty Participants	• IP address, device information, log data, your use of the App, ads you have displayed or viewed, settings made in your account • Applicable only in Romania: the voice of Users, by recording conversations, if they contact the Call Center for further information about the App or for various requests and in order to improve our services	• Art. 6(1)(f) GDPR - Legitimate interest

Marketing Communications (general or based on profiles or location) through the communication channels chosen by the relevant users	• Private Customers • Loyalty Participants Not applicable to Business Users	name, email address, telephone number.	• Article 6(1)(a) GDPR – consent
Profiling and personalized offers	• Private Customers • Loyalty Participants Not applicable to Business Users	charging and transaction history, loyalty activity, Application usage, preferences, survey responses, communication choices and location data where separately permitted.	• Article 6(1)(b) GDPR – based on performance of the Benefits Program contract where profiling is necessary to allocate Benefits requested under the Benefits Program; • Article 6(1)(a) GDPR - consent for personalized marketing communications and marketing-related location use
Benefits Program membership and administration: • checking whether an OMV MyStation loyalty account already exists; • linking an existing account; • creating a loyalty account where requested; administering participation; allocating and managing benefits; and preventing duplicate accounts.	• Private Customers • Loyalty Participants	email address used as the linking identifier; name, surname, gender, country, city, date of birth, account identifiers, charging or transaction history, number of loyalty points, loyalty points used, coupons and benefits, as applicable, shopping history, buying habits and preferences, values or type of products or services purchased	• Article 6(1)(b) GDPR – taking pre-contractual steps at the applicant's request and performance of the Benefits Program contract.
Financial-accounting management of the benefits granted via the benefits Program	• Loyalty Participants	transaction data, benefits data	• Art. 6(1)(c) GDPR - fulfilment of legal obligations
Location Services	• Business Users • Private Customers • Loyalty Participants	location data	• Art. 6(1)(a) GDPR – Consent

We usually collect data from you through the Application. For business charging, we may also receive your email address from the business customer that requests the service for you. You must nevertheless log in to the Application and accept the applicable terms and conditions before using the charging service.
Loyalty data comes from you and your use of either applications and is recorded in the common loyalty backend of the Application and OMV MyStation.

We do not make solely automated decisions with legal or similarly significant effects.

4. Personalized marketing consent and profiling

4.1. Marketing communications and marketing-related profiling are offered only to Private Customers and Loyalty Participants. They are not offered to Business Users in connection with their business-related EV charging account. Private Customers and Loyalty Participants may expressly consent to general or personalized marketing activities, including personalized offers and personalized marketing communications based on registration data, charging, the analysis of their purchase history, survey and Application data. This helps us identify specific preferences of the Private Customer/Loyalty Participants and offer more relevant products or services.

Private Customers and Loyalty Participants may give separate, freely given consent for each relevant purpose and communication channel including email, push notifications, profiling, location-based marketing and non-essential third-party analytics services. Depending on the functionality offered in the Application, separate choices may be presented for:

- general marketing by email;
- general marketing by push notification;
- personalized marketing based on profiling;
- personalized marketing based on real-time or approximate location;
  non-essential analytics SDKs.

No consent option will be preselected. The relevant processing will begin only after the user has made an affirmative choice. We retain appropriate records of the consent choice, including the purpose, channel, wording presented and time of the choice.

Where a Private Customer or Loyalty Participant consents to personalized marketing, we may combine charging and transaction history, Application and loyalty use, stated preferences, survey responses, communication choices, engagement with previous campaigns and, where separately permitted, real-time or approximate location data.

The analysis may consider factors such as:

- the type, value, date, frequency and location of charging sessions or purchases;
- the EV charging station used;
- products or services purchased;
- coupons or benefits earned or used;
- date of birth, city or other optional registration details;
- preferred communication channels;
- survey responses; and
- interaction with previous offers or campaigns.

Authorised personnel determine the audience-selection criteria, campaign rules, communication channels and relevant offers or benefits. The systems may then assess the available data and place users into segments matching those criteria. For example, a user who has consented to push-notification marketing and separately enabled location for marketing may receive an offer concerning an EV charging point located in a Controller's filling station (OMV or OMV Petrom) near the user's location.

Refusing marketing consent does not affect registration, account maintenance, EV charging services or benefits available independently of marketing consent. It only prevents relevant marketing communication, consent-based profiling, location-based marketing or non-essential analytics processing.

Refusing or withdrawing marketing consent does not affect participation in the Benefits Program or benefits available independently of that consent.

Private Customers and Loyalty Participants may withdraw consent at any time, separately for each purpose and communication channel, through the Application's Privacy Settings or Permissions section, by using the unsubscribe or opt-out option in a marketing message, or by contacting us under Section 7.
A user may, for example, stop email marketing communications while continuing to receive push-notifications, or withdraw location-based marketing permission without closing the account.
Choices saved in the Application apply to future processing once recorded. Requests submitted by email or post will be implemented without undue delay. Withdrawal does not affect the lawfulness of processing carried out before withdrawal and does not close the account, prevent EV charging or terminate participation in the Benefits Program.
After withdrawal, we will stop the relevant marketing communication, marketing-related profiling, location-based marketing or non-essential analytics processing. Strictly functional messages may continue where necessary to operate the account, administer EV charging or loyalty services, provide security notifications or communicate service changes. Essential diagnostic processing may also continue where it is based on our legitimate interest in maintaining the security, stability and reliability of the Application.
For linked accounts, eMotion withdrawal affects only the corresponding eMotion purpose; separately maintained OMV MyStation preferences must be changed there unless stated otherwise.

4.2. To perform the Benefits Program Contract, we may analyse purchase, loyalty, transaction, location, benefit and optional profile data against staff-defined criteria to allocate requested benefits. Systems identify eligible participants to grant benefits solely by virtue of their status as participants, or according to eligibility criteria which may involve an automated decision-making process. This may include an analysis of:

a) their preferences and consumption habits resulting from the purchase history (type and quantity of products purchased, amount of purchase, filling station from which the purchase was made, date of purchase) which may be considered, individually or in combination with other data collected from the Loyalty Participant;
b) data provided by the Loyalty Participant at the time of registration in the Benefits Program, such as date of birth, place of residence, the option for certain communication channels (email, push notifications);
c) their loyalty activity to determine eligibility for discounts, coupons, rewards or other benefits.

For the Benefits Program, the Controller may analyse data generated through the eMobility Application to create participant segments and determine eligibility for personalized benefits. The analysis may use relevant purchase and loyalty activity, including transaction value and frequency, products or services purchased, the location and date of a purchase, benefits earned or used, and optional registration details, preferences or survey responses provided by the Loyalty Participant. Authorised personnel define the eligibility criteria and the benefits to be granted. The relevant systems then identify Loyalty Participants who meet those criteria.
Profiling for marketing communications is separate and will take place only where the Loyalty Participant has expressly consented to receive those communications.
This profiling supports benefit allocation and personalization but has no legal or similarly significant effects through solely automated effect decisions. We apply safeguards and assess privacy risk.
Applying for or declining the Benefits Program does not affect access to eMotion EV charging services. A Private Customer who does not activate the loyalty option in the Application or join the Benefits Program will not receive loyalty points, coupons, rewards or other program-specific benefits.

5. How long do we retain your data?

We retain your personal data for as long as necessary to provide the eMotion Application and related charging services, maintain your account and fulfil the purposes described in this Privacy Notice.
Generally, we retain your personal data while the account is active and up to 12 months after closure. After 24 months of inactivity, we may notify you and close the account unless use resumes.
You may request deletion in the Application. After any stated confirmation period, we delete or anonymise the data unless a pending matter or legal claims require retention. Loyalty data remains while program participation is active through either application.

6. With whom do we share your data?

We share only necessary data with providers supporting the Application, charging, payments and loyalty.
Current providers include ChargePoint (charging backend), Codibly (application provision and maintenance) and Comarch (loyalty backend, account linking and benefit administration).
Other recipients may include payment and IT, support and advisers, relevant OMV Group entities and public authorities. They receive only the needed data and act as processors or controllers, as applicable.
Some of our service providers may process personal data in countries outside the European Economic Area ("EEA"). Where personal data is transferred outside the EEA, we ensure that appropriate safeguards are implemented in accordance with applicable data protection laws. These safeguards may include the use of Standard Contractual Clauses approved by the European Commission or other transfer mechanisms recognized under the GDPR.

7. Your Rights

Under the GDPR, you may access and correct your data; request erasure or restriction where legal conditions apply; withdraw consent without affecting earlier lawful processing; object to legitimate-interest processing and direct marketing; avoid solely automated decisions with legal or similarly significant effects; and receive portable data where processing is automated and based on consent or contract.
Complaint with supervisor authorities: you can lodge a complaint with the National Supervisory Authority for Personal Data Protection according to the details under **Section 8** below.
To exercise your rights, please contact us using the contact details provided in **Section 9** of this Privacy Notice.

8. Country-Specific Information

Additional local provisions are available in the country policies below:

Austria: See the General Data Privacy Policy at: Data protection is important to us | OMV.com
Information regarding the Austria National Supervisory Authority for Personal Data Protection can be found at: Österreichische Datenschutzbehörde

Slovakia: See the General Data Privacy Policy at www.omv.sk/gdpr-info
Information regarding the Office for Personal Data Protection of the Slovak Republic can be found at www.dataprotection.gov.sk

Romania: See the General Data Privacy Policy at https://www.omv.ro/ro-ro/omv-in-romania/nota-de-informare.

Information regarding the Romanian National Supervisory Authority for Personal Data Protection (ANSPDCP) can be found at www.dataprotection.ro.

Hungary: See the General Data Privacy Policy at: https://www.omv.hu/hu/adatvedelmi-tajekoztato
Information regarding the Hungarian National Authority for Data Protection and Freedom of Information can be found at: https://naih.hu/

9. Contact Details and exercise of your rights

For questions or rights requests, use the contacts below.
Austria: privacy@omv.com
Romania: submit the form at: https://www.omv.ro/ro-ro/omv-in-romania/nota-de-informare, email privacy@petrom.com, or write to the Data Protection Officer, OMV Petrom Marketing S.R.L., 22 Coralilor Street, Infinity Building, 1st Floor, Oval B, Sector 1, Bucharest. We may verify your identity.
Slovakia: submit the form at www.omv.sk/gdpr-info, email privacy.sk@omv.com or write to the Data Protection Officer, OMV Slovensko s.r.o., Einsteinova 25, 851 01 Bratislava. We may verify your identity
Hungary: privacy.hu@omv.com

***

Latest update of this Policy: October 2026

To ensure the proper functioning, security, performance monitoring, analytics, and monetization of our eMotion application, we use and integrate various third-party technologies, services, and software components provided by external partners.

For the purposes of the GDPR, we act as the Data Controller, while the providers of these technologies and services act either as Data Processors (where they process personal data solely on our behalf and in accordance with our instructions) or as independent or joint Controllers (where they determine the purposes and means of processing, including where they combine data with information obtained from other sources for their own purposes). For further information regarding the processing carried out directly by a provider, including retention periods, international data transfers, and the exercise of data subject rights in relation to such processing, please consult the provider's privacy notices.

No non-essential technologies or services (including analytics, telemetry, or advertising-related services) will be activated or permitted to collect your data unless and until you provide your explicit consent through our Consent Management Platform.

Below you can find the complete list of third-party services, technologies, and integrations used in this Application.

-

1. **Essentials**

-

Mapbox (essential analytic)

Provider (processor) : Mapbox Inc., 740 15th Street NW, 5th Floor, Washington, DC 20005, USA

Parent Company: Mapbox Inc. (USA)

Purpose: rendering map tiles

Category: Location Services

Data Processed:

- Mapbox processes map geo-coordinates that may be centered around user´s location in case user´s device permission consents are granted
- IP address
- device characteristics
- operating system
- application version
- timestamps
- request-related diagnostic information

Legal Basis:

Article 6(1)(b) GDPR (contract performance): The processing of map-related data through Mapbox is necessary for the performance of the contract pursuant to Article 6(1)(b) GDPR, as the mapping functionality is required to enable users to locate charging stations, display charging stations infrastructure and provide the map and use location features-based functionalities requested by the user through the application.

Technology Used: SDK integration

Website: https://www.mapbox.com/

Retention period:

Data is kept only as long as needed to provide, secure and monitor the map service, then deleted or anonymised. Mapbox processes your data for the duration necessary to provide the map functionality and related security, diagnostics and performance services. Technical map-request, telemetry and diagnostic data are retained only for limited operational purposes and are deleted or anonymised once no longer required.

Additional Information:

When a map is displayed, Mapbox receives the requested map area and limited technical data needed to deliver and secureby the service. If location is allowed on the device, the GPS-based location coordinates are sent to Mapbox in order to centre the map around the user's current position and provide nearby charging stations; otherwise, if location permissions are not granted, the application displays a predefined default map area and the device's GPS coordinates are not sent. Mapbox may process telemetry, diagnostics, security or service-improvement data for its own purposes under its privacy terms.

International data transfers:

Mapbox Inc. is located in the United States. Where personal data is transferred outside the European Economic Area (EEA), appropriate safeguards are implemented in accordance with applicable data protection laws.

Firebase Cloud Messaging (essential analytic)

Provider (processor) : Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland

Parent Company: Google LLC (USA)

Purpose: Push notification delivery, device messaging

Category: Messaging Services

Data Processed:

The data processed is technical and related to notification delivery. It includes:

- Installation Identifier: A pseudonymous identifier for this installation of the app, used to route notifications to the correct device.
- Device Token (unique, pseudonymous identifiers): A pseudonymous token issued by Google for this installation, which we store on our own systems to send notifications.
- App instance ID
- Notification delivery metadata (delivery status, timestamps)
- Device information (OS, version, device type)

IP address and network connection information required for message delivery and service security.

Legal Basis

Article 6(1)(b) GDPR (**contract** performance**)** when the processing is necessary to deliver service-related push notifications concerning the user's account, charging sessions, charging status and updates, operational alerts. Where push notifications are used for marketing purposes, processing is based on the user's consent under Article 6(1)(a) GDPR.

Technology Used: SDK integration

Website: https://firebase.google.com/products/cloud-messaging

Retention period: The FCM Firebase Cloud Messaging (FMC) device token is retained by the application backend only for as long as necessary to deliver push notifications. Upon account deletion, all FCM tokens linked to the deletedaccount are deleted as part of the account deletion process, unless temporary retention is required by law or for security or /audit purposes.

Additional Information:

FCM delivers operational and, where consented, marketing push notifications. A pseudonymous token links the app installation to the correct device; it is stored by the application and routed through Google. Google processes the notification content and limited technical delivery data only to transmit messages and maintain service security and reliability. Notifications stop and the registration is removed when the user signs out or disables them. FCM is a messaging service used to deliver push notifications to the user's mobile device which may include charging-

session updates, charging completion notifications, account-related messages, service notifications, security alerts and other operational communications necessary for the provision of the eMotion services.
International data transfers: Google Ireland Limited may engage Google LLC and affiliated entities located outside the European Economic Area (EEA) for the provision of the messaging service. Where personal data is transferred outside the EEA, appropriate safeguards are implemented in accordance with applicable data protection laws.

Firebase Crashlytics (essential analytic)

- **Provider (processor) :** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland
- **Parent Company**: Google LLC (USA)
- **Purpose**: Crash reporting, app stability monitoring, debugging support
- **Category**: Diagnostics
- **Data Processed**: crash traces, device information (OS, version, device type), annonymized user ID and app usage data at the time of the crash

Legal Basis:
The processing is necessary for the Controller's legitimate interest (Article 6(1)(f) GDPR (legitimate interests): processing is limited to maintaining the security, stability, reliability and technical diagnostics needed to keep performance of the eMotion application secure, stable, identifying and reliable, fix software defects, prevent service disruptions and improve performance ensuring an appropriate user experience. The processing is limited to diagnostic and technical information necessary for these purposes.
Technology Used: SDK integration
Website: https://firebase.google.com/products/crashlytics
Retention period:
CrashFirebase Crashlytics keeps crash stack traces, extracted minidump data, and related identifiers (including Crashlytics Installation UUIDs and Firebase installation identifiers) for 90 days before removal from live and backup systems begins.
Additional Information:
Crashlytics automatically sends pseudonymised technical reports when the app crashes or has a non-fatal error. Reports may include crash traces, installation identifiers, app and operating-system versions, device type and state, orientation, memory, disk space and root/jailbreak status. The data is used to investigate recurring issues, prioritise fixes and improve application stability; it is not used to directly identify users. Firebase Crashlytics enables the investigation of the incident and improvement of the application's stability. Crash reports contain technical diagnostic information and pseudonymized identifiers. They are not used to directly identify users.
International data transfers: Google Ireland Limited may engage Google LLC and affiliated entities located outside the European Economic Area (EEA) in connection with the provision of Firebase Crashlytics. Where personal data is transferred outside the EEA, appropriate safeguards are implemented in accordance with applicable data protection laws.

Chargetrip (essential analytic)
Provider: Chargetrip B.V., Singel 542, 1017 AZ Amsterdam, Netherlands
Parent Company: Chargetrip B.V. (EU)
Purpose: EV route planning, charging station recommendations, range prediction, navigation optimization
Category: Routing & Navigation Services
Data Processed:

- Vehicle catalog reference id

- Battery state-of-charge percentages
- Route coordinates

Legal basis:

Article 6(1)(b) GDPR (contract performance). The processing is necessary to provide the Route Planner functionality requested by the user, including route calculation, charging-stop recommendations, range estimates and navigation-related services within the eMotion application.

Technology Used: backend sub-processor

Website: https://www.chargetrip.com

Retention period:

RouteChargetrip processes route-planning data as long as necessary to calculate and provide the requested EV route and related charging-stop recommendations, range prediction and navigation optimisation.

Additional Information:

Chargetrip provides EV route planning only when the user opens Route Planner. The application sends the selected route points, vehicle model, battery charge and other technical parameters needed to calculate routes, charging stops, range and charging needs. The data is pseudonymised, used only for these calculations, and is not used for cross-session tracking or behavioural analytics. The service is activated only when a user chooses to use the Route Planner functionality. If the user does not use the Route Planner functionality, no route-planning information is transmitted to Chargetrip.

International data transfers: Chargetrip B.V. is established in the European Union (Netherlands). Any transfers of personal data outside the European Economic Area (EEA), where applicable, are carried out in accordance with applicable data protection laws and appropriate safeguards.

2. **Non-essentials**

Firebase Analytics (optional)

Provider: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland

Parent Company: Google LLC (USA)

Purpose: App usage analytics, feature performance measurement, user engagement insights

Category: Analytics Services

Data Processed:

- Pseudonymous app instance ID
- Event data (screen views, feature interactions, session duration)
- Device information (OS, version, device type, language settings)
- App performance metrics (load times, errors, navigation flows)
- Region-level location (country-level only; no precise GPS)

Technology Used: SDK integration

Legal basis: consent under Article 6(1)(a) GDPR. Firebase Analytics is activated only after consent in the app's privacy settings. Consent may be withdrawn at any time without affecting prior processing or access to core app functions; future analytics collection then stops.

Retention Period:

Retention depends on purpose. IP addresses are normally kept for 30 days, but may be retained longer where needed for security or fraud investigations or legal compliance.

Website: https://firebase.google.com/products/analytics ▪

Additional Information:

With consent, Firebase Analytics collects pseudonymised app-use and performance data, such as screen views, feature interactions, navigation, session duration, device and operating-system details, language, country-level location and an app-instance ID. It is used to measure use, identify usability and performance issues and improve the app. It is not intended to collect names, contact details or other direct identifiers.
International data transfers: Google Ireland Limited may engage Google LLC and affiliated entities located outside the EEA for the provision of the analytics service. Where personal data is transferred outside the EEA, appropriate safeguards are implemented in accordance with applicable data protection laws.

Mapbox Telemetry (optional)
Provider: Mapbox Inc., 740 15th Street NW, 5th Floor, Washington, DC 20005, USA ▪
Parent Company: Mapbox Inc. (USA)
Purpose: Technical usage monitoring, performance optimization, map delivery quality improvement. This may include information about map movement, zooming, route display performance and approximate movement patterns used to improve map services.
Category: Diagnostics & Performance
Data Processed:

- Tile request metadata (tile ID, zoom level, load status)
- Map interaction events (zoom, pan, rotation)
- Rendering and network errors
- Performance metrics (latency, load times, number of tiles requested)
- Device information (OS, version, device type, screen resolution)
- IP address (temporary, for routing and load balancing) ▪

Legal basis: consent under Article 6(1)(a) GDPR. Mapbox Telemetry is optional and starts only after consent in the app's privacy settings. Consent may be withdrawn at any time without affecting prior processing or use of the map; future telemetry collection then stops.
Technology Used: SDK integration
Website: https://www.mapbox.com/legal/privacy
Retention Period:
Mapbox stores personal data for so long as it is needed to fulfill the purposes for which it was collected. In determining how long to retain personal data, Mapbox considers the amount, nature and sensitivity of the data, the potential risk of harm from unauthorized use or disclosure of the data, the purposes for which personal data is processed, applicable legal requirements, and Mapbox's legitimate interests. The purposes for which Mapbox processes data may dictate different retention periods for the same types of data. For example, Mapbox retains IP addresses for 30 days and after such time, in select instances, may need to extend such retention period for an investigation based on its legitimate interests to secure its products and services, prevent fraud and for legal compliance purposes.
Additional Information:
With consent, Mapbox Telemetry collects pseudonymised map-interaction, viewport, tile-request, error, performance, device, operating-system, IP-address and related location signals. The data is used only for diagnostics, map quality, performance and service improvement, not by the Controller to identify users or create advertising profiles. Telemetry is off by default, does not affect map access and stops when consent is withdrawn. Mapbox Telemetry is a diagnostic and performance-monitoring service used to understand how map functionality performs within the application and to improve map rendering quality, responsiveness and service reliability.
International data transfers:

Mapbox Inc. is located in the United States. Where personal data is transferred outside the European Economic Area (EEA), appropriate safeguards are implemented in accordance with applicable data protection laws.