PRIVACY POLICY

LOOP-PARK — Mobile application — Luxembourg

Version 1.1 — Effective as of 01/11/2026

This English version is a translation of the French original. In the event of any discrepancy between the language versions, the French version shall prevail.

Main changes in version 1.1: approval of reservations by the Owner, Monthly Rental paid in Instalments, new payment methods, messaging between Users, search alerts, clarifications on data shared between Users and on retention periods.

1. Scope

This Privacy Policy explains how Loop-Park ("Loop-Park", "we", "us" or "our") collects and processes your personal data in connection with our Loop-Park services. This Privacy Policy applies to our website, our mobile application and any other online service provided by us that refers to this Privacy Policy (together, the "Service").

Please read this privacy policy carefully. If you have any questions about this policy, please do not hesitate to contact us: we will do our best to answer them.

2. Data controller

Loop-Park S.à r.l.-S

9, rue du Laboratoire

L-1911 Luxembourg

E-mail: legal@loop-park.lu

RCS Luxembourg: B297871

Loop-Park acts as data controller within the meaning of Regulation (EU) 2016/679 (GDPR).

3. Data collected

3.1 Identification data

- Surname and first name
- E-mail address
- Telephone number
- Postal address (where applicable)
- Profile photo (optional)

3.2 Account data

- Login e-mail address
- Usage history
- 6-digit OTP code sent at login (not retained after validation)

3.3 Reservation and listing data

- Reservation dates and times
- Address of the parking space
- Precise GPS coordinates of the space (stored via PostGIS in Supabase)
- Licence plate of the Driver's vehicle

- Make and model of the Driver's vehicle
- History of reservations and cancellations
- Ratings and reviews (rating from 1 to 5, comments)
- Photos of spaces published by Owners
- Reservation Requests, including those declined, expired or withdrawn
- Vehicles registered in the profile and vehicle declared for each Reservation
- Access instructions and codes for the space provided by the Owner
- Instalments of Monthly Rentals and status of each payment
- Private or professional status of the Owner
- Version of the General Terms and Conditions accepted, date and time of each acceptance
- Search alerts created by the Driver (area and radius)

Privacy note: the precise address of a space (including the street number) is only disclosed to the Driver after confirmation of the reservation and payment (a listing only shows the postcode and the street). EXIF metadata in photos (which may contain GPS coordinates) is removed when the files are processed.

3.4 Geolocation data

When the User uses the proximity search, the application may access the device's geographical position, subject to the permission granted via the iOS or Android settings. This data is used to display nearby spaces and is not stored permanently. It is transmitted to Mapbox (base maps) and used via the PostGIS function search_available_slots_nearby.

3.5 Payment data

Payments are processed by Stripe Technology Europe Limited. Loop-Park does not store any bank card number — tokenisation is carried out exclusively by the Stripe SDK on the User's device, without passing through Loop-Park's servers. For Drivers, Loop-Park stores the Stripe customer identifier and the payment method identifier required for the Pre-authorisation and the charging of Instalments, as well as the brand, the last four digits and the expiry date of the card; for Owners, the Stripe Connect account identifier. The full card number and the security code are never transmitted to Loop-Park. Payments by Apple Pay, Google Pay, Link and Revolut Pay are processed by Stripe and by the provider concerned, in accordance with their own privacy policies.

3.6 Technical data

- IP address
- Connection logs (authentication, Edge Functions, administration console)
- Device type and operating system
- JWT session tokens (managed by the Supabase Auth SDK)

3.7 Fraud prevention data

- Behavioural analysis
- Proportionate identity checks (KYC carried out by Stripe for Owners — Loop-Park does not receive any identity document)
- Tax information required by the DAC7 directive (EU 2021/514), entered by the owner in the "Tax information" section of the profile.

3.8 Communications and support

- Messages exchanged between Users via the Application's messaging service, accessible only during a confirmed Reservation
- Exchanges with support, reports and disputes, including attachments (supporting documents, photos)
- Notification preferences and technical push notification tokens
- Choice regarding receipt of Loopers community news

4. Sensitive personal data

In principle, we will not ask you to provide sensitive personal data. If we do request such information, we will explain why we are asking for it, how we will use it and the legal basis on which we rely.

5. Purposes of processing

The data is used for the following purposes:

- creating and managing accounts;
- performing reservations;
- managing payments;
- managing Reservation Requests and their approval by the Owner;
- charging the Instalments of Monthly Rentals and sending reminders before each charge;
- putting Users in contact via the messaging service during a confirmed Reservation;
- sending alerts about new spaces;
- keeping proof of acceptance of the General Terms and Conditions;
- marketing communications, in particular Loopers community news;
- fraud prevention;
- platform security;
- dispute management;
- compliance with tax obligations (DAC7);
- user support.

6. Legal bases

Processing is based on:

- performance of the contract, for purposes including (i) creating and managing accounts; (ii) performing reservations; (iii) managing payments; (iv) managing Reservation Requests, Instalments, messaging and alerts; (v) user support;
- a legal obligation, for purposes including (i) fraud prevention; (ii) platform security; (iii) compliance with tax obligations (DAC7);
- legitimate interest, for purposes including (i) platform security; (ii) fraud prevention; (iii) platform analysis and service improvement; (iv) personalisation and ranking of listings; (v) dispute management; (vi) keeping proof of acceptance of the General Terms and Conditions;
- consent, for any marketing communications.

7. Retention periods

- Account management data: duration of the contractual relationship + 5 years.
- Accounting and transaction data: 10 years (legal obligations).
- Fraud prevention data: 12 months.
- Data relating to a dispute: duration of the dispute + statutory periods.
- Marketing communications data: until consent is withdrawn.
- Proof of acceptance of the General Terms and Conditions: duration of the contractual relationship + 5 years.
- Messages between Users: deleted when the account is deleted.
- Exchanges with support and attachments: deleted when the account is deleted, or, in the event of a dispute, duration of the dispute + statutory periods.
- Payment method identifiers: until the last Instalment or until deleted by the User.
- Push notification tokens: until logout or account deletion.
- Search alerts: until deleted by the User.

When we no longer need the personal data we have collected about you, we delete or anonymise it. If we anonymise your personal data (so that it can no longer be associated with you), we may use this information indefinitely without further notice to you.

8. Recipients of data

Data may be transmitted to the following categories of recipients, strictly within the scope of their respective tasks and for the purposes described in this Privacy Policy:

8.1 Providers established in the European Union

- Brevo SAS: transactional e-mails for OTP, confirmations, reservation requests, reminders and Instalment charge notices (Paris, France) — data: e-mail address, first name and surname, Reservation details (Space address, dates, amounts, access instructions); and, with the User's consent, subscription to the community news list
- Stripe Technology Europe Limited: payments, KYC of Owners (Dublin, Ireland)

8.2 Providers established outside the European Union

- Mapbox Inc. (United States): base maps — data: IP address, approximate location (transfer governed by the EU-US Data Privacy Framework)
- Firebase Cloud Messaging, Google LLC (United States): pseudonymised technical tokens (transfer governed by the EU-US Data Privacy Framework)
- Supabase Pte. Ltd. (Singapore), supported by Supabase, Inc. (United States) for technical support: database, files, Edge Functions — data hosted in the EU (Ireland — West EU, AWS eu-west-1); access possible from third countries for support purposes (transfer governed by the European Commission's standard contractual clauses)

8.3 Information shared between Users

In order to provide the parking service, certain information is shared between Drivers and Owners:

- Geolocation information and location of the space
- Information exchanged during a reservation
- Ratings and information relating to account reliability

More specifically: before confirmation, the Driver sees the area of the Space, without the street number, as well as the Owner's first name, status and rating; an Owner who must approve a Reservation Request sees the Driver's first name, length of membership, rating and licence plate. After confirmation, the Driver receives the exact address, the access instructions and the Owner's first name. Both parties can then communicate via the messaging service until the end of the Reservation. No contact details are disclosed if a Reservation Request is declined or expires.

8.4 Disclosure to authorities

Personal data may also be disclosed:

- to the competent tax authorities: data required by the DAC7 directive (EU 2021/514);
- to judicial authorities: where required by law.

9. Hosting and technical infrastructure

The technical infrastructure of the Loop-Park application is provided by:

- Data and media (PostgreSQL database, photo files, Deno/TypeScript Edge Functions): hosted by Supabase (Supabase Pte. Ltd.) in a data centre in Ireland (West EU — AWS eu-west-1).

Users' data is hosted exclusively within the European Union; occasional access from third countries is possible under the conditions described in Article 11.

10. Data Protection Officer (DPO)

At present, Loop-Park is not required to appoint a data protection officer within the meaning of Article 37 of Regulation (EU) 2016/679, as our processing activities and our current user base do not reach the threshold that would make such an appointment mandatory. We undertake to review this assessment at regular intervals and whenever there is a substantial change in our processing activities, our operations or the size of our user base. Any question relating to the protection of personal data may be addressed to: legal@loop-park.lu

11. Transfers outside the European Union

Some of the third-party providers used by Loop-Park are located outside the European Union. These transfers are governed in accordance with the requirements of the GDPR:

- Stripe Technology Europe Limited (Dublin, Ireland — EU): may transfer certain data to Stripe group entities in the United States — Privacy Policy: https://stripe.com/fr-lu/privacy
- Mapbox Inc. (United States): base maps, IP address and approximate location — governed by the EU-US Data Privacy Framework.
- OpenStreetMap Foundation / Nominatim (United Kingdom): geocoding data — the United Kingdom benefits from an adequacy decision of the European Commission.
- Firebase Cloud Messaging, Google LLC (United States): pseudonymised technical tokens (transfer governed by the EU-US Data Privacy Framework).
- Supabase Pte. Ltd. (Singapore) and Supabase, Inc. (United States): data hosted in the EU (Ireland — West EU), but the support team may access data from third countries for maintenance operations — transfer governed by the European Commission's standard contractual clauses — Privacy Policy: https://supabase.com/privacy.

In all cases, Loop-Park ensures that appropriate safeguards provide a level of protection equivalent to that guaranteed within the European Union.

12. Security

Loop-Park implements the following technical and organisational security measures:

12.1 Encryption at rest

- PostgreSQL database encrypted with AES-256 (AWS RDS on the Supabase side)
- Files and photos encrypted with AES-256 (AWS S3 on the Supabase Storage side)

12.2 Encryption in transit

- HTTPS / TLS 1.2 minimum on all data flows: mobile application, administration console, third-party APIs
- Signed Stripe webhooks (HMAC verification) to prevent event spoofing

12.3 Bank data

- Card numbers never pass through Loop-Park's servers — tokenisation is carried out exclusively by the Stripe SDK on the device (PCI DSS Level 1 compliance via Stripe)

12.4 Access control

- PostgreSQL Row Level Security (RLS): each user only accesses data corresponding to their role (driver / owner / administrator)
- Administration console protected by 3 levels: (1) e-mail OTP via Supabase Auth, (2) server-side verification of the administrator role, (3) IP address whitelist on the Hetzner Cloud firewall

12.5 Privacy protection

- Precise address of the space (street number) hidden before confirmation of the reservation

- EXIF metadata of photos removed during processing

12.6 Backups and continuity

- Automatic daily Supabase backups
- Point-in-Time Recovery (PITR) — 7-day restore window (Pro plan)
- Application logging: authentication, Edge Functions, notifications, cancellations

13. Automated decisions

We use certain automated processes where necessary to provide and administer our services. These processes may include:

- suspending or restricting an account when our systems detect repeated or serious breaches of our General Terms and Conditions, or any other suspicious or fraudulent activity;
- immediate confirmation of a Reservation for Spaces that do not require the Owner's approval;
- automatic cancellation of a Reservation Request to which the Owner has not responded within 24 hours;
- automatic charging of the Instalments of a Monthly Rental;
- automatic termination of a Monthly Rental after 48 hours without settlement of a declined payment;
- automatic calculation and application of deductions, refunds and transfers in the event of late cancellation (in accordance with the cancellation policy in force);
- ranking and display of listings based on factors such as location, availability, reliability and history.

Where an automated decision produces legal effects or similarly significantly affects you, we rely on Article 22(2)(a) GDPR, as the processing is necessary for the performance of our contract with you or for taking pre-contractual steps at your request. Where Article 22 GDPR applies, we implement appropriate safeguards to protect your rights. You have the right to obtain human intervention, to express your point of view and to contest the decision. No account suspension or restriction producing legal effects or similarly significant effects will be definitively implemented without an effective human review. Requests for human review may be sent to legal@loop-park.lu. We will acknowledge receipt of your request as soon as possible and provide a reasoned response within a reasonable time.

14. Cookies and trackers

This article describes how we use cookies and similar technologies. It explains what these technologies are, why we use them and your rights to control their use.

14.1 What is a tracker?

A tracker is a technical identifier placed on or read from your device (smartphone, tablet), enabling the operation, security or analysis of the Application. In a mobile application, these trackers may take the form of:

- session identifiers,
- device identifiers,
- third-party SDKs (Software Development Kits),
- technical logs.

14.2 Categories of trackers

14.2.1 Strictly necessary trackers (no consent required)

These trackers are essential for the Application to function and do not require the User's prior consent. They enable in particular:

- authentication and session management;
- securing access to accounts;
- fraud prevention;
- the proper technical functioning of the application;
- the management of secure payment transactions.

14.2.2 Performance and analytics trackers

These trackers collect information about how visitors use our Application, the most frequently visited pages and any error messages received from web pages. They help us improve our Application. Their purpose is:

- analysing use of the application;
- improving performance;
- detecting technical anomalies;
- improving usability and user experience.

Should Loop-Park use analytics or audience measurement trackers that are not strictly necessary, they would only be activated after obtaining the User's prior consent.

14.2.3 Functional trackers

These trackers enable the Application to offer enhanced features and personalisation, such as remembering your preferences. They are only activated after obtaining the User's prior consent.

14.2.4 Advertising or targeting trackers

These trackers are used to deliver advertisements more likely to match your interests. They are also used to limit the number of times an advertisement is shown and to measure the effectiveness of advertising campaigns. As of the date of this policy, Loop-Park does not use any advertising or retargeting trackers, unless otherwise notified to the User when they are activated. Should such trackers be activated in the future, they would be subject to:

- specific information;
- prior consent;
- a simple withdrawal mechanism, accessible at any time.

14.3 List of trackers used

As of the date of this policy, Loop-Park uses trackers that are strictly necessary for operation and security. The Application currently does not use any advertising, retargeting or audience measurement tools. It only uses:

1. Strictly necessary trackers (no consent required)

#	Tracker / Cookie	Provider	Purpose	Duration	Data transmitted	Transfer outside EU
1	Supabase Auth session tokens (JWT: sb-access-token / sb-refresh-token)	Supabase Pte. Ltd. — hosted in Ireland — West EU (AWS eu-west-1)	Authentication, session maintenance, account security	Duration of the session + automatic expiry	User identifier, e-mail address, session identifier, authentication role, access token and refresh token, token issue and expiry information.	Yes (support access from third countries) — standard contractual clauses
2	Stripe SDK (flutter_stripe)	Stripe Technology Europe Limited, Dublin, Ireland	Secure payment, fraud prevention, SCA/PSD2 strong authentication. Card tokenisation takes place on the	Duration of the transaction	Payment card data transmitted directly to Stripe, payment method identifier, transaction amount and currency, payment status, customer	Depending on the case

			device — no bank data passes through Loop-Park's servers. Payment methods: cards, Apple Pay, Google Pay, Link and Revolut Pay.		and connected account identifiers, and technical data used for fraud prevention. Loop-Park does not store any complete payment card data.	
3	Mapbox SDK (flutter_map + Mapbox tiles)	Mapbox Inc., United States	Display of the interactive map, viewing available spaces	Duration of the session	IP address, approximate geographical location, tile requests	Yes (United States) — DPF
4	Brevo — transactional e-mails	Brevo SAS, 55 rue d'Amsterdam, 75008 Paris, France	Login OTP, reservation confirmations, reservation requests, Instalment charge notices, end-of-reservation reminders	Kept until the account is deleted	E-mail address, first name, surname, Reservation details (Space address, dates, amounts, access instructions)	No
5	Administratio n console session cookies (sb-* via @supabase/ss r — Next.js)	Supabase Pte. Ltd. — Loop-Park administration console domain only (not accessible to end users)	Authentication of Loop-Park administrators	Duration of the administra tor session	Administrator user identifier, e-mail address, role and permissions, session identifier, access token and refresh token, token issue and expiry information.	Yes (support access from third countries) — standard contractu al clauses
6	Firebase Cloud Messaging SDK	Google LLC, United States	Sending push notifications (reminders, reservation requests, messages)	Until logout or account deletion	Device notification token (pseudonymised), operating system	Yes (United States) — DPF

2. Analytics trackers

None — not used in the current version of the Application.

3. Advertising trackers

None — not used.

14.4 Consent management

When the Application is used for the first time, a screen allows the User to accept or refuse non-essential trackers. Consent is freely given, specific, informed and revocable. Preferences can be changed at any time in the application settings. Refusing non-essential trackers does not prevent access to the main features. Only essential cookies will be used to provide you with the necessary features of the Application. You can manage your preferences in: Settings → Privacy → Tracker management (accessible at any time within the application) and contact us at: legal@loop-park.lu.

14.5 Retention period

Strictly necessary trackers are only retained for the period strictly necessary to achieve their purpose. Trackers placed on the basis of the User's prior consent are retained for a maximum of thirteen (13) months from the time they are placed.

14.6 Updates

We may change our use of cookies and tracking technologies in order to improve our services or comply with legal requirements. Any new non-essential tracker requiring consent will not be placed or activated before valid consent has been obtained from the user via the consent management mechanism described in Article 14.4. Continued use of the Platform does not constitute consent where consent is required by law.

15. Your rights

In accordance with the GDPR, you have:

- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restriction of processing;
- the right to object;
- rights relating to automated individual decision-making, as set out in Article 13 of this Privacy Policy;
- the right to data portability.

Exporting your data is not yet available directly in the Application; it is provided to you upon request sent to legal@loop-park.lu, within the time limit indicated below. Where processing is based on consent (in particular for marketing communications and Loopers community news), the User may withdraw their consent at any time, without affecting the lawfulness of processing carried out before such withdrawal. Withdrawal may be made:

- via the unsubscribe link in communications;
- via the account settings;
- or by contacting legal@loop-park.lu.

You can exercise your rights at: legal@loop-park.lu. Loop-Park undertakes to respond to any request to exercise rights within one (1) month of receipt. This period may be extended by a further two (2) months in the case of a complex request, after informing the User within the initial period. To exercise your rights: legal@loop-park.lu — stating your name, your account e-mail address and the precise nature of your request.

16. Complaints

You may lodge a complaint with:

Commission nationale pour la protection des données (CNPD) — Luxembourg

15, Boulevard du Jazz — L-4370 Belvaux

Website: www.cnpd.lu · Tel.: +352 26 10 60 1

You may also contact the supervisory authority of your country of residence if you reside in another Member State of the European Union.

17. Account deletion and right to erasure (Art. 17 GDPR)

Any User may request the deletion of their account and the erasure of their identifying data. Access in the application: My space → Account → Delete my account.

17.1 Phase 1 — Request (immediate and automatic)

The request triggers a grace period of thirty (30) days during which the User may withdraw it. During this period, the creation of new listings and new reservations is blocked. Deletion is not possible

while a Reservation or a Monthly or hourly Rental is ongoing or upcoming; it does not bring forward the end of commitments made to the other party.

17.2 Phase 2 — Execution (within 5 working days of the end of the grace period)

- Cascading anonymisation of identifying data: profile → anonymous identifier, listings archived, reservations / reviews / tokens anonymised
- Deletion of the associated Stripe Connect account (if the User is an Owner)
- Unsubscription from the Brevo contact list

17.3 Data retained after deletion

- Financial and transaction data: retained for 10 years under an anonymised identifier (accounting law, DAC7), then automatically purged
- In the event of an ongoing dispute: retained for the duration of the dispute + statutory periods
- Proof of acceptance of the General Terms and Conditions: duration of the contractual relationship + 5 years, then deleted

18. Updates

This privacy policy may be amended from time to time to reflect changes in legal requirements, industry standards or our activities. In the event of a material change to this privacy policy that may affect your rights or the way we process your personal data, we will inform you by visible means, such as e-mail, notifications on the website or any other appropriate channel. We will also indicate the effective date of the updated policy at the top of the document. Changes do not apply retroactively to reservations already made. New versions are announced in the Application and remain available under Account.

For material changes to our privacy policy that require the User's consent under applicable data protection legislation, we will seek your express consent (opt-in) before implementing these changes. You will be able to review the updated policy and give your consent before any change takes effect.