PrePark Data Retention Schedule

INTERNAL - Version 1.0 | Last updated 14 September 2026

1. Principles

- Keep personal data only for as long as necessary for the purpose collected.
- Apply the shortest workable retention period consistent with legal, accounting, security and dispute needs.
- Restrict access to archived records and delete/anonymise them securely at the end of the period.
- Document exceptions and legal holds.

2. Retention schedule

Record type	Default retention	Reason / notes
Customer account profile	Active account + up to 6 years after closure where linked to transactions; otherwise delete/anonymise sooner	Contract, claims, fraud prevention and support history.
Host account and listing history	Active relationship + 6 years after closure	Contracts, claims, listing disputes and regulatory evidence.
Booking records, invoices, payments, refunds and Stripe IDs	6 years after the end of the relevant financial year / transaction period	Accounting, tax, contracts and legal claims.
HMRC digital-platform seller due-diligence/reporting records	5 years after the end of the relevant reportable period	Current HMRC digital-platform record-keeping requirement.
Vehicle registration and permit/access records	Normally retained with the booking record where needed for disputes; minimise visibility after booking	Booking delivery, permit disputes and enforcement evidence.
Reusable permit/key/fob deposit records	6 years after resolution where linked to a financial transaction/dispute	Financial and contractual evidence.
Customer/Host support messages	3 years after case closure; up to 6 years if linked to a contractual or legal dispute	Support, complaints and claims.
Formal complaints and dispute decisions	6 years after closure	Defence of claims and consistency of dispute handling.
SAR / data-rights request records	3 years after closure	Demonstrate compliance and handle follow-up.
Personal data breach log	6 years from closure of incident	Accountability and regulatory evidence.
Security/audit logs	Normally 12 months; longer if linked to an incident, fraud case or legal hold	Security monitoring and investigation.
Marketing preferences / consent records	While marketing continues plus a reasonable evidence period; retain minimal suppression record after opt-out	Demonstrate consent/opt-out and prevent re-marketing.

Record type	Default retention	Reason / notes
Cookie consent records	Normally 3 years or until superseded where needed to evidence consent	PECR/consent evidence; review with consent platform settings.
Unsuccessful Host verification material	Delete promptly once no longer required, unless retained for fraud/security reasons	Data minimisation.

3. Deletion and anonymisation

Deletion should include production databases, accessible exports and operational copies where reasonably practicable. Backup data may expire through normal backup rotation provided it is protected from ordinary use and not restored except for legitimate disaster recovery.

4. Ownership and review

The person responsible for data protection should review this schedule at least annually and when PrePark introduces new data types, suppliers, features or legal obligations.