ELOCITY A CONNECTED EV WORLD

Elocity Technologies Inc. — Smart Electric Vehicle Charging Technology Company

Data Retention Policy

1. Principles

Elocity collects EV charging session data, driver identity and contact information, payment records, diagnostic logs, and vehicle details. We retain personal information only as long as necessary for the purposes for which it was collected or as required by law, in accordance with PIPEDA, Quebec Law 25, U.S. state privacy laws (including CCPA/CPRA), and the GDPR where applicable. When data is no longer needed, we permanently delete it or irreversibly anonymise it; anonymized aggregates (with no personal identifiers) may be retained for analytics. We review our holdings against this schedule regularly and purge data that has outlived its purpose, including data of accounts inactive for extended periods.

2. Retention Schedule

Data category	Retention period
Account and identity data (name, contact)	Life of account + 90 days after deletion request or closure
Charging session data (time, location, kWh)	Life of account; anonymized thereafter for analytics
Payment and transaction records	7 years
Carbon credit measurement data	Program verification period + 7 years
Diagnostic and equipment logs	24 months
Support communications	36 months
Video surveillance (where Elocity-operated)	30–90 days unless retained for an incident
Marketing consents and suppression lists	Duration of consent + proof of consent retained
Breach/incident register (Quebec Law 25)	Minimum 5 years from incident

3. Deletion Requests

Verified deletion requests are honoured in all jurisdictions: Canada (offered as good practice under PIPEDA and required in Quebec under Law 25), the United States (CCPA/CPRA and similar state laws), and GDPR regions (right to erasure). We acknowledge and respond within statutory timelines — generally 30 days under PIPEDA/Law 25 and GDPR, and 45 days under CCPA with one 45-day extension where reasonably necessary and notified. Complete removal from active systems and backups is targeted within 90 days of verification. Data we must retain by law (for example, financial records) is

kept to the minimum necessary, isolated, and where feasible de-identified. Service providers and sub-processors are instructed to delete corresponding data.

4. Disposal Methods

Electronic personal information is deleted using secure-erasure methods appropriate to the medium; physical records, where any exist, are cross-cut shredded. Anonymization removes all direct and indirect identifiers so individuals can no longer be identified, in line with regulatory guidance.