ELOCITY A CONNECTED EV WORLD

Elocity Technologies Inc. — Smart Electric Vehicle Charging Technology Company

PRIVACY POLICY

Elocity Technologies Inc. ("Elocity," "we," "us") protects personal information in compliance with applicable privacy laws, including Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), Quebec's private-sector privacy act as amended by Law 25, the BC and Alberta Personal Information Protection Acts, the California Consumer Privacy Act as amended by the CPRA, India's Digital Personal Data Protection Act, 2023, and the EU/UK GDPR. Our core commitment: your personal information is stored and processed in the country or region where it is collected, and it stays there.

1. Definitions

"Personal information" means information about an identifiable individual; it excludes properly aggregated or de-identified information that cannot reasonably re-identify you. "Driver" means an individual who uses Elocity-connected charging or the HIEV app. "Site Host" means a building owner, condominium or strata corporation, property manager, fleet, or other organization hosting Elocity-connected chargers. "Visitor" means someone who browses our websites without an account. "Charging session data" means session start/end time, duration, energy (kWh), charger ID, tariff, and amounts charged.

2. Who This Policy Covers

This policy applies to Drivers, Site Hosts and their authorized personnel, and Visitors, across our websites, the HIEV mobile app, the HIEV CPMS portal, and connected charging hardware. It does not cover third-party websites we link to, which have their own policies.

3. What We Collect

Audience	Personal information collected
Drivers	Name, email, phone, address; account credentials; minimal payment identifiers via our payment platform (we never store full card numbers); charging session data; vehicle make/model (optional); device data (IP, device ID, OS) and GPS location only if you enable location services; support interactions; information you volunteer (surveys, licence plate or date of birth only where a specific program requires it, with notice).
Site Hosts	Business contact details of authorized personnel; portal credentials and access logs; banking details for settlement payouts (collected for electronic funds transfer, passed to our payment platform, verified by call-back, and not retained on primary servers where avoidable); agreement and billing records.
Visitors	Cookies and similar technologies, web server logs (IP, pages viewed, time). No account information is required to browse.

We do not knowingly collect personal information from anyone under 18; if you are under 18, please do not use our services.

4. How We Use Personal Information

- Provide and manage accounts, charging services, and settlement with Site Hosts;
- Process payments and payouts; detect and prevent fraud; secure our network (including OCPP security profiles and SOC 2-aligned controls);
- Provide 24/7 bilingual (English/French) customer support;
- Send service notices; send marketing only with consent compliant with Canada's Anti-Spam Legislation (CASL), always with an unsubscribe link;
- Produce aggregated, de-identified analytics to improve services and to report to Site Hosts, utilities, and regulators;
- Participate in carbon credit and utility programs you or your Site Host enrol in (s. 6);
- Meet legal, tax, and regulatory obligations, including in corporate transactions.

We rely on express consent for marketing, location services, and any technology that identifies, locates, or profiles you; implied consent or recognized legal bases for service delivery, fraud prevention, and legal compliance. We never use personal information for materially different purposes without your consent.

5. Automated Decision-Making

We do not make decisions that produce legal or similarly significant effects about you using exclusively automated means. Where automation assists a decision (for example, fraud screening), a human reviews any adverse outcome on request, and Quebec residents will be informed as Law 25 requires.

6. Sharing and Disclosure

We do not sell personal information for money. We share it only as follows, and only to the extent necessary:

- **Site Hosts — aggregate only.** Settlement statements and host reports are site-aggregated (sessions, kWh, amounts).
- **Service providers / sub-processors:** payment processing, cloud hosting in-region (e.g., AWS, Microsoft Azure, Oracle Cloud as applicable), authentication, IT and customer support — each bound by data processing agreements; a current sub-processor list is available from the Privacy Officer on request.
- **Carbon credit and clean fuel programs:** where chargers are enrolled, charging session data is reported to Environment and Climate Change Canada, provincial regulators (e.g., BC LCFS), and accredited validation/verification bodies to create and audit credits. Reporting is limited to what the regulation requires.
- **Utilities and demand-response programs:** where you or your Site Host enrol in a utility managed-charging program, we share the program-required charging data with the utility under program rules, with notice at enrolment.
- **Roaming partners** as needed to deliver charging you request on partner networks;
- **Affiliates, professional advisors, and parties to corporate transactions** (with notice if practices materially change); and law enforcement or authorities where required by law.

Third parties receiving aggregated, de-identified data receive no personal information.

7. Data Residency and International Access

Elocity stores and processes personal information within the country or region where it is collected. Canadian personal information is stored and processed in Canadian cloud regions and remains in Canada;

Indian personal data remains in India; EU/UK data is protected by appropriate safeguards including standard contractual clauses.

On a limited basis, authorized Elocity support or engineering staff may access data remotely. Where such staff are outside the country of storage, access occurs entirely within Elocity-controlled secure environments on the same in-country infrastructure: the data is viewed through controlled, logged, audited connections — never transferred, downloaded, or copied to another country. Access is restricted to the minimum necessary, protected by multi-factor authentication and confidentiality obligations, and remains subject to Elocity's accountability. For Quebec residents, any such remote access is treated as a communication outside Quebec and is covered by a privacy impact assessment (s. 12).

8. Cookies and Similar Technologies

Category	Purpose	Your control
Strictly necessary	Sign-in, security, fraud prevention, core site functions.	Cannot be disabled; no consent needed.
Functional	Remember language and preferences.	Browser settings / our cookie banner.
Analytics	Measure usage to improve services.	Cookie banners opt-out; browser settings.
Advertising	Limited interest-based advertising on our own services.	We honour the Global Privacy Control (GPC) signal; opt out via banner, GPC, or industry tools (Google Ad Settings, NAI).

Disabling cookies may limit some features. Where sharing with advertising platforms is “sharing” under the CPRA, you may opt out (s. 13).

9. Retention and Security

Record type	Indicative retention
Account profile	Life of account + 90 days after verified deletion request, then deleted or anonymized
Charging session and settlement records	7 years (financial, tax, and audit obligations)
Carbon credit program data	Per program regulation (CFR/LCFS verification periods)
Support tickets	3 years
Web logs and analytics	13 months or less

Exact periods are set in our Data Retention Policy. We protect personal information with TLS in transit and encryption at rest, role-based access with multi-factor authentication, SOC 2-aligned hosting with firewalls and intrusion detection, staff training, and contractor confidentiality. No system is impenetrable: if a breach creates a real risk of significant harm, we notify affected individuals and regulators within legal timelines and record it in our breach register.

10. Your Rights

Subject to applicable law, you may access and correct your personal information; request deletion; object to or restrict certain processing (including direct marketing); request a portable copy; and withdraw consent at any time without affecting prior processing. We never discriminate against you for exercising rights. Contact

the Privacy Officer (s. 16); we respond to verifiable requests within statutory timelines (generally 30 days under PIPEDA and Law 25; 45 days under the CCPA, extendable once), free of charge unless requests are manifestly excessive. Drivers can also delete their account directly in the HIEV app.

Country and region-specific terms. Sections 11–15 apply in addition; where they differ, the regional term prevails for users in that region.

11. Canada (PIPEDA and provincial laws)

We collect, use, and disclose personal information only for purposes a reasonable person would consider appropriate, with knowledge and consent except where the law permits otherwise. Canadian data remains in Canada (s. 7). Complaints: our Privacy Officer first; then the Office of the Privacy Commissioner of Canada or your provincial regulator (OIPC BC, OIPC AB).

12. Quebec (Law 25)

We have designated a person in charge of the protection of personal information (the Privacy Officer); we conduct privacy impact assessments for projects involving personal information and any communication outside Quebec; we maintain a confidentiality incident register and notify the Commission d'accès à l'information of incidents presenting a risk of serious injury; technologies that identify, locate, or profile you activate only with express consent; this policy is posted in French.

13. United States (CCPA/CPRA and state laws)

California residents may opt out of “sale” or “sharing” (including cross-context behavioural advertising) via the “Do Not Sell or Share My Personal Information” link, GPC, or by contacting us; and have rights to know, access, correct, delete, and limit use of sensitive personal information, without discrimination. We honour equivalent rights for residents of other states with similar laws.

14. India (DPDP Act, 2023)

We process digital personal data on the basis of consent or recognized legitimate uses. You may access a summary of your data, request correction and erasure, nominate a representative, and seek grievance redressal from our Grievance Officer at privacy@elocitytech.com; unresolved grievances may go to the Data Protection Board of India. Indian personal data is stored and processed in India and remains in India (s. 7).

15. EU/EEA, UK, and Other Regions

EU/EEA and UK users have GDPR/UK GDPR rights (access, rectification, erasure, restriction, portability, objection, complaint to a supervisory authority); transfers are protected by appropriate safeguards including standard contractual clauses. Users in the UAE, Saudi Arabia, Singapore, the Philippines, Australia, and other jurisdictions: we comply with applicable local laws (UAE PDPL, Saudi PDPL, Singapore PDPA, Philippine DPA 2012, Australian Privacy Act/APPs) and honour the rights they grant. Data is stored in the country or region of collection where law requires, otherwise in the nearest Elocity-approved hosting region, and remains there per Section 7.

16. Contact, Changes, Accessibility

Privacy Officer, Elocity Technologies Inc.

Unit 23A, 156 Duncan Mill Road, North York (Toronto), Ontario M3B 3N2, Canada — privacy@elocitytech.com — +1 (416) 384-1919. We may update this policy; revisions are posted with a new effective date and version number, and material changes are notified by email or in-app message before they take effect. This policy is available in English and French and in accessible formats on request.