Rightcharge Security Overview

Policy Owner: CTO
Review Frequency: Annual
Last Reviewed: Jan 2026

External Security Summary — Jan 2026

Rightcharge Limited provides EV charging management services, including the Electric Fuel Card programme for home, public and workplace charging. Because charging session and energy tariff data can reveal personal preferences and behaviours, we treat it as personal data and protect it accordingly. This document summarises the security, privacy and resilience measures that underpin our service. It is intended for customers, partners and prospective customers carrying out due diligence; the full policy set referenced here is available on request.

Certifications and Compliance

Rightcharge is Cyber Essentials Plus certified, demonstrating independently verified technical security controls across our systems, infrastructure and operations.

Rightcharge maintains a security and privacy programme designed to support compliance with applicable data protection requirements, including UK GDPR. Our security programme is governed by an umbrella Information Security Policy supported by dedicated standards covering encryption, data protection, data retention and business continuity, each subject to a defined annual review cycle.

Framework	Status	Detail
Cyber Essentials	Certified — whole organisation	Certified 7 Nov 2025 (IASME / Round Cyber); recertification due Nov 2026
UK GDPR / DPA 2018	Compliant	Registered UK data controller; documented data protection programme
NIST 800-207	Aligned	Zero-trust principles applied across service architecture

Infrastructure and Data Residency

The Rightcharge platform is hosted on Amazon Web Services. Customer personal data is stored in the UK and Ireland, with our primary data store running in AWS DynamoDB in the EU-West-2 (London) region. Where any personal data is transferred outside the UK or European Economic Area, we apply appropriate safeguards such as approved standard contractual clauses. Our cloud infrastructure uses built-in redundancy and geographically separate data centres for replication, and our architecture supports national data residency requirements where these apply.

Encryption and Key Management

All data is encrypted in transit and at rest. Web and API traffic is protected with TLS 1.3 or higher, with HTTP Strict Transport Security (HSTS) enforced. Data at rest is encrypted to the AES-256

standard using AWS Key Management Service with customer-managed keys, giving us fine-grained control over encryption policy. Key material is held in hardware security modules, key usage is logged and monitored, and keys are rotated automatically on a defined schedule.

Rightcharge never stores user passwords. Authentication is delegated to OAuth 2.0-compliant identity providers, and any transient credentials such as reset tokens are securely hashed and expire within minutes. Access to energy supplier systems is handled exclusively through tokenisation: tokens are encrypted, stored in a secure secrets store isolated from customer data and application code, scoped to least privilege, and subject to usage limits and expiry.

Access Control

Our service is designed around zero-trust principles aligned with the NIST 800-207 framework, requiring continuous verification of all actors within the infrastructure to limit the impact of any compromise. Access to systems and data follows the principle of least privilege with role-based access control, and all operational staff are subject to separation of duties with multi-factor authentication enforced. Sensitive personal data is segmented from non-sensitive information, classified to a high confidentiality standard by default, and accessible only to authorised personnel whose access is reviewed against job responsibilities.

Secure Development and Vulnerability Management

All software is built and maintained under a secure system development lifecycle. This includes secure coding practices, static and dynamic code analysis, application security reviews at design, development and deployment stages, input validation and output encoding to prevent injection and cross-site scripting attacks, and assessment of third-party dependencies with a maintained software bill of materials. Development, test and production environments are segregated, and all changes to production pass through formal change control.

Systems are scanned for vulnerabilities before production deployment and periodically thereafter, and annual penetration tests verify the effectiveness of our encryption and tokenisation controls. Discovered vulnerabilities are remediated under a documented plan of action, and all systems are kept at vendor-supported patch levels with critical patches applied within defined timeframes. Networks are segmented in tiers separating internet-facing systems, high-sensitivity systems and user segments, and intrusion detection and monitoring systems alert our incident response personnel to indications of compromise.

Logging and Monitoring

All operations on our data stores, including access to encrypted tables, are logged via AWS CloudTrail and reviewed regularly for anomalies. Applications produce audit logs capturing security-relevant events such as access attempts, configuration changes and failures, and these logs are centralised, protected and retained in line with our retention schedules.

Business Continuity and Disaster Recovery

A maintained Business Continuity Plan protects critical functions, data and services during disruption. Daily and weekly backups of critical systems are taken with offsite storage, and a structured backup retention schedule keeps daily backups for 30 days, weekly backups for six months, monthly backups for one year and annual backups for seven years. Data recovery is tested quarterly, the wider plan is exercised at least annually through simulated disruptions, and recovery time and recovery point objectives are defined for critical functions. Post-incident reviews feed improvements back into the plan.

Data Retention and Secure Disposal

Data is retained only as long as necessary for the purpose for which it was collected, against a documented retention schedule covering customer, employee, financial and operational data. At the end of its retention period, data is securely deleted across all databases, storage systems and backups using industry-standard destruction methods, including cryptographic erasure, so that it cannot be recovered or reconstructed. Disposal is recorded for compliance verification, and users are notified once deletion is complete.

Privacy and Data Subject Rights

Rightcharge Limited is the controller of personal information collected via our website and services, and we support all rights afforded under UK data protection law: access, rectification, erasure, restriction, portability, objection, and rights relating to automated decision-making. Tariff data is captured only with the user's active, explicit consent, which can be withdrawn at any time, and we collect only the information required to provide the service. We support verified data subject access requests, including where we process data on behalf of business customers. Payment card and bank details are handled entirely by our licensed payment provider, Stripe; Rightcharge never receives or stores them.

People and Suppliers

All staff receive security awareness training within 30 days of joining, reinforced at least annually, and roles with access to sensitive information are subject to suitability checks where lawful. Access is revoked immediately on separation. Third-party providers are engaged only after due diligence on their security and data protection practices, operate under formal Data Processing Agreements, and remain subject to ongoing oversight including security reviews and audit rights.

Incident Response

Rightcharge maintains documented incident response procedures with designated response teams responsible for assessing, containing and mitigating incidents. In the event of a breach affecting personal data, we notify affected individuals, regulatory authorities and other relevant stakeholders in accordance with legal requirements, and supplier access tokens are immediately invalidated and regenerated. Every incident concludes with a root-cause review to prevent recurrence.

Contact

For security questions or to request copies of our underlying policies, contact engineering@rightcharge.co.uk. For privacy queries and data subject requests, contact customercare@rightcharge.co.uk.

Registered address: 86-90 Paul Street, London, England, EC2A 4NE | Company registration: 11957019 | VAT number: 420 8425 21