Policy Owner: CTO
Review Frequency: Annual
Last Reviewed: October 2025

Data Protection Policy

1. Introduction

1.1. Purpose

This Data Protection Policy sets forth the principles and guidelines for safeguarding the confidentiality, integrity, and availability of data processed by Rightcharge Limited. It aims to ensure compliance with relevant data protection laws and regulations while maintaining the trust of our users.

1.2. Scope:

This policy applies to all employees, contractors, and third parties who have access to the data processed by Rightcharge Limited, regardless of the location or method of access. It encompasses all aspects of data handling, including collection, storage, processing, and sharing.

2. Data Collection and Use

2.1. Purpose Limitation

We collect and process charge session and tariff data from users for the purpose of billing organisations accurately for the services utilized and discussing funds to drivers home energy accounts or to chargepoint operators and to display an aggregated or individual 360 view of a users/fleets charging .Any additional use of this data beyond billing purposes requires explicit consent from the users.

2.2. Data Minimization

We limit the collection of data to what is strictly necessary for billing purposes and ensure that it is accurate, relevant, and up-to-date. We do not collect or retain any unnecessary or excessive data.

2.3. Consent

Prior to collecting any data from users, we obtain their explicit consent and inform them about the specific purposes for which their data will be processed. Users have the right to withdraw their consent at any time.

3. Data Security

3.1. Confidentiality

We implement robust technical and organizational measures to ensure the confidentiality of the data processed, including access controls, encryption, and role-based permissions. Access to sensitive data is restricted to authorized personnel only.

3.2. Integrity

We maintain the accuracy and integrity of the data by implementing measures to prevent unauthorized access, data tampering, or corruption. This includes regular data validation checks and audit trails to track any changes to the data.

3.3. Availability

We ensure the availability of the data by implementing redundant systems, backup procedures, and disaster recovery plans. This helps prevent data loss or downtime due to system failures or unexpected events.

4. Data Sharing and Transfers

4.1. Third-party Providers

We may share data with third-party service providers only to the extent necessary to provide our services, such as payment processing or cloud hosting. When engaging third-party providers for services such as payment processing or cloud hosting, we conduct thorough due diligence to assess their data protection practices and ensure alignment with our own standards.

4.1.1. Vendor Assessment:

Prior to engaging a third-party service provider, we assess their capabilities, expertise, security measures, and compliance with relevant data protection regulations. This assessment includes evaluating the provider's data security protocols, certifications, and track record in handling sensitive information.

4.1.2. Data Processing Agreements:

Before sharing any user data with third-party providers, we establish formal agreements, such as Data Processing Agreements (DPAs), that clearly outline the terms and conditions governing the processing of data. These agreements specify the purposes for which the data will be processed, the security measures to be implemented, and the responsibilities of each party regarding data protection.

4.1.3. Security and Confidentiality

We require third-party providers to implement robust security measures to safeguard the confidentiality, integrity, and availability of the data they process on our behalf. This includes encryption of data in transit and at rest, access controls, regular security audits, and employee training on data protection best practices.

4.1.4. Monitoring and Oversight:

We maintain ongoing oversight of third-party providers to ensure compliance with our data protection standards. This includes regular reviews of their security posture, performance evaluations, and audits of their data handling processes. Any deviations from agreed-upon security measures are promptly addressed and remediated.

4.2. International Transfers

If data is transferred to countries outside the European Economic Area (EEA) or other regions with strict data protection laws, we ensure that appropriate safeguards are in place to protect the data, such as standard contractual clauses approved by the relevant authorities.

5. Data Retention

5.1. Retention Period

We retain data only for as long as necessary to fulfill the purposes for which it was collected, as outlined in our data retention policy. This period may vary depending on the nature of the data and legal requirements. Upon cancellation of user accounts, we retain the associated data for a period of one year, unless otherwise required by law or regulatory requirements.

5.1.1. Justification

The one-year retention period allows us to address any potential disputes, inquiries, or billing-related issues that may arise following the cancellation of user accounts. It also provides a reasonable timeframe for users to reactivate their accounts if they choose to do so within that period.

5.1.2 Backup Retention

The backup retention policy mandates that daily backups are retained for 30 days, while weekly backups are kept for six months. Monthly backups are stored for one year, and annual backups are preserved for seven years or longer if required by legal or regulatory obligations. This structured approach ensures compliance, data availability, and efficient storage management.

5.2. Data Disposal

Following the expiration of the retention period, user data is securely deleted from all systems and platforms across our infrastructure. This deletion process is conducted in a manner that ensures the irretrievable removal of data and prevents any unauthorized access or disclosure.

5.2.1. Cross-Platform Deletion:

Rightcharge Limited employs a systematic approach to data deletion, ensuring that user data is removed from all databases, storage systems, backups, and any other repositories where it may have been stored. This includes any redundant or obsolete copies of the data maintained for backup or archival purposes.

5.2.2. Secure Data Destruction

We utilize industry-standard data destruction methods, such as cryptographic erasure or physical destruction of storage media, to ensure that deleted data cannot be recovered or reconstructed by unauthorized parties. This helps mitigate the risk of data breaches or unauthorized access to sensitive information.

5.3. User Notification

Upon the completion of the data deletion process, users are notified that their data has been permanently removed from our systems in accordance with our data retention and disposal policies. This transparency reaffirms our commitment to protecting user privacy and maintaining compliance with applicable data protection laws and regulations.

6. Data Subject Rights

6.1. Access and Rectification

Users have the right to access their personal data held by Rightcharge Limited and request corrections or updates if it is inaccurate, incomplete, or outdated. We provide users with accessible mechanisms, such as user account portals or dedicated request forms, to exercise these rights. Upon receiving a valid request, we promptly respond and take necessary actions to rectify any inaccuracies or discrepancies in the data.

6.2. Erasure

Users have the right to request the erasure of their personal data under certain circumstances, such as when it is no longer necessary for the purposes for which it was collected, if they withdraw their consent, or if they object to the processing and there are no overriding legitimate grounds for the processing. Rightcharge Limited acknowledges and respects this right and implements procedures to facilitate the erasure of user data upon request, subject to legal obligations and exceptions.

6.3. Objection and Restriction

Users can object to the processing of their personal data or request restrictions on its processing in certain situations, such as if they believe the data is inaccurate or unlawfully processed. We consider and address these objections in accordance with applicable legal requirements.

7. Compliance and Enforcement

7.1. Compliance

Rightcharge Limited maintains robust mechanisms for monitoring and ensuring compliance with data protection laws and regulations, including but not limited to the General Data Protection Regulation (GDPR) and other applicable frameworks. This includes regular audits, assessments, and reviews of our data processing activities, policies, and procedures to identify and address any areas of non-compliance or improvement opportunities.

7.2. Training and Awareness

We prioritize ongoing training and awareness programs for all employees, contractors, and third parties who handle personal data on behalf of Rightcharge Limited. These programs provide comprehensive guidance on data protection principles, legal requirements, and best practices to ensure that personnel understand their roles and responsibilities in safeguarding user data. Regular training sessions, updates, and communications help maintain a culture of data protection and privacy awareness throughout the organization.

7.3. Reporting

Rightcharge Limited maintains robust incident response procedures to address any breaches of data protection or security incidents promptly and effectively. Employees are trained to recognize and report incidents through established channels, and designated response teams are responsible for assessing, containing, and mitigating the impact of incidents. In the event of a data breach or incident, Rightcharge Limited promptly notifies affected individuals, regulatory authorities, and other relevant stakeholders in accordance with legal requirements and our internal incident response protocols. Post-incident reviews and analysis are conducted to identify root causes, lessons learned, and opportunities for improvement to prevent future incidents.

8. Policy Review

This Data Protection Policy is subject to periodic review and may be updated as necessary to reflect changes in technology, business practices, or legal requirements. Any updates or revisions to the policy will be communicated to all relevant stakeholders and made available on our website or internal portals.

9. Conclusion

Protecting the privacy and security of user data is paramount to Rightcharge Limited. This Data Protection Policy serves as a commitment to maintaining the highest standards of data protection and ensuring the rights and freedoms of individuals whose data we process. By

adhering to the principles and guidelines outlined in this policy, we strive to build and maintain trust with our users and stakeholders.

10. Document history

Version	Date Approved	Approved By	Brief Description
1.0	11/4/2024	Kevin Ikelle	Document creation
1.2	28/05/2024	Kevin Ikelle	Modification to Backup Retention section
1.3	28/11/2024	Kevin Ikelle	Modification to Subprocessors
1.4	10/01/2025	Kevin Ikelle	Yearly Review