Data Processing Agreement

Recharge - Template v1.0

Last updated 21 July 2026

This document is a template for customer organisations. Processor company registration fields marked in brackets should be completed once incorporation details are confirmed. Request a countersigned copy at support@recharge.app.

This Data Processing Agreement ("DPA") forms part of the agreement between the customer organisation identified below ("Customer" or "Controller") and the provider of the Recharge service ("Recharge" or "Processor") for the Recharge annual leave planning and team coordination platform (the "Service").

This DPA reflects the parties' agreement with regard to the processing of personal data under the UK GDPR, the EU GDPR, and the UK Data Protection Act 2018 (together, "Data Protection Law"). It is intended to meet the requirements of Article 28 of the UK/EU GDPR.

By executing an order form, creating an organisation workspace, or otherwise accepting Recharge's Terms of Service, Customer agrees to this DPA. A countersigned copy may be requested by emailing support@recharge.app.

1. Definitions

Terms used but not defined in this DPA have the meaning given in Data Protection Law or in Recharge's Terms of Service. "Personal Data", "Processing", "Controller", "Processor", "Data Subject", "Personal Data Breach", and "Supervisory Authority" have the meanings in UK/EU GDPR. "Sub-processor" means any Processor engaged by Recharge to process Customer Personal Data.

"Customer Personal Data" means Personal Data that Customer (or its authorised users) submits to the Service, or that Recharge otherwise processes on Customer's documented instructions in providing the Service.

2. Roles of the parties

Customer is the Controller of Customer Personal Data. Recharge is the Processor. Each party will comply with its obligations under Data Protection Law. Nothing in this DPA relieves either party of those obligations.

Where a Customer user connects a personal (non-organisation) account, Recharge may also act as an independent Controller for that personal account data, as described in the Privacy Policy. This DPA governs organisation-workspace processing where Customer is Controller.

3. Scope, nature, and purpose of processing

Recharge will process Customer Personal Data only to provide, maintain, secure, and support the Service; to fulfil Customer's documented instructions (including configuration of leave policies, approvals, integrations, and exports); and as required by applicable law.

The subject matter, duration, nature, purpose, types of Personal Data, and categories of Data Subjects are set out in Schedule 1. Processing continues for the term of Customer's subscription and any residual period needed for deletion or return under this DPA.

4. Customer instructions

Recharge will process Customer Personal Data only on Customer's documented instructions, unless required to do otherwise by UK or EU law (in which case Recharge will inform Customer of that legal requirement before processing, unless the law prohibits such notice).

Customer's instructions are documented in this DPA, the Terms of Service, the Privacy Policy, and Customer's use and configuration of the Service (including integrations Customer enables). Customer warrants that its instructions are lawful and that it has a valid legal basis for the processing.

5. Confidentiality

Recharge will ensure that persons authorised to process Customer Personal Data are bound by confidentiality obligations (contractual or statutory) and receive appropriate data-protection training.

6. Security

Taking into account the state of the art, costs of implementation, and the nature, scope, context, and purposes of processing, as well as the risk to Data Subjects, Recharge will implement and maintain appropriate technical and organisational measures to protect Customer Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Those measures are summarised in Schedule 3 and on Recharge's Security page, and may be updated provided the overall security posture is not materially reduced.

7. Sub-processors

Customer provides a general written authorisation for Recharge to engage Sub-processors to process Customer Personal Data for the purposes of delivering the Service. The current list of Sub-processors is in Schedule 2. The live list published at /security#subprocessors controls in case of conflict with this Schedule.

Recharge will impose data-protection obligations on each Sub-processor that are no less protective than those in this DPA, to the extent applicable to the Sub-processor's services. Recharge remains responsible to Customer for each Sub-processor's performance of those obligations.

Recharge will give Customer at least 30 days' prior notice of any intended addition or replacement of a Sub-processor (via email to organisation admins, in-product notice, or an update to the published Sub-processor list). Customer may object on reasonable data-protection grounds within that period. If the parties cannot resolve an objection, Customer may terminate the affected Service as its sole remedy.

8. International transfers

Customer Personal Data may be processed in the United Kingdom, the European Economic Area, and other countries where Recharge or its Sub-processors operate. Where Data Protection Law requires a transfer mechanism for transfers of Customer Personal Data out of the UK or EEA, Recharge will ensure an appropriate safeguard is in place (for example, an adequacy decision, the UK International Data Transfer Agreement / Addendum, or the EU Standard Contractual Clauses), and will flow down equivalent protections to Sub-processors as required.

9. Assistance with Data Subject rights

Taking into account the nature of the processing, Recharge will assist Customer by appropriate technical and organisational measures, insofar as possible, in fulfilling Customer's obligations to respond to Data Subject requests under Data Protection Law (access, rectification, erasure, restriction, portability, and objection).

Where a Data Subject contacts Recharge directly regarding Customer Personal Data, Recharge will promptly redirect the request to Customer, unless legally required to respond directly. Customer remains responsible for responding to Data Subjects.

10. Breach notification

Recharge will notify Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data. The notice will include, to the extent then known: a description of the nature of the breach; the categories and approximate number of Data Subjects and records concerned; the likely consequences; and the measures taken or proposed to address the breach.

Recharge will reasonably cooperate with Customer's investigation and any required notifications to Supervisory Authorities or Data Subjects. Notification under this clause is not an admission of fault or liability.

11. DPIAs and prior consultation

Taking into account the nature of processing and information available to Recharge, Recharge will provide reasonable assistance to Customer with data protection impact assessments and prior consultations with Supervisory Authorities that relate to Customer's use of the Service.

12. Audit and information rights

Recharge will make available to Customer information necessary to demonstrate compliance with this DPA, and will allow for and contribute to audits, including inspections, conducted by Customer or an independent auditor mandated by Customer, subject to reasonable confidentiality, security, and scheduling requirements.

Unless required by a Supervisory Authority or following a confirmed Personal Data Breach attributable to Recharge, audits are limited to once per rolling twelve-month period, on at least 30 days' written notice, during normal business hours, and without unreasonably disrupting Recharge's operations. Customer may satisfy audit rights in the first instance via Recharge's security documentation, questionnaire responses, and (where available) third-party reports.

13. Return and deletion

Upon termination or expiry of the Service, or upon Customer's written request, Recharge will, at Customer's choice, delete or return Customer Personal Data (including existing copies), unless UK or EU law requires storage. Customer may export organisation data from the Service while the subscription is active. Deletion will complete within a reasonable period after termination, consistent with Recharge's retention practices described in the Privacy Policy.

14. Customer responsibilities

Customer is responsible for: (a) the accuracy and lawfulness of Customer Personal Data submitted to the Service; (b) providing any notices and obtaining any consents required for the processing; (c) configuring the Service and integrations appropriately; and (d) not submitting special-category data to the Service except where Customer has a lawful basis and has configured the Service accordingly (for example, certain sick-leave records).

15. Liability

Each party's liability under this DPA is subject to the limitations and exclusions in the Terms of Service, except to the extent such limitations are prohibited by Data Protection Law. Nothing in this DPA limits either party's liability for death or personal injury caused by negligence, fraud, or any other liability that cannot be limited by law.

16. Term, precedence, and governing law

This DPA takes effect on the date Customer first accepts it (or the date of countersignature, if later) and continues until Recharge ceases processing Customer Personal Data. If there is a conflict between this DPA and the Terms of Service on a data-protection matter, this DPA prevails. This DPA is governed by the same law and jurisdiction as the Terms of Service, unless Data Protection Law requires otherwise.

Recharge may update this DPA to reflect changes in Sub-processors, security measures, or legal requirements. Material adverse changes will be notified with reasonable advance notice. Continued use of the Service after the effective date constitutes acceptance, except where Customer terminates under the objection rights in clause 7.

Schedule 1 - Details of processing

Subject matter

Personal Data processed in providing the Recharge leave-management and team-coordination Service to Customer's organisation workspace.

Duration

For the term of the subscription and any period required for deletion, return, dispute resolution, or legal retention.

Nature and purpose

Hosting, storage, retrieval, transmission, display, and analysis of leave and related workplace data to operate bookings, approvals, allowances, coverage, notifications, digests, AI leave suggestions, calendar/chat sync, MCP access Customer enables, billing administration, and support.

Types of Personal Data

Account identifiers (name, email); organisation membership and roles; leave records (dates, types, notes, approval status, allowance, work pattern); integration identifiers and tokens needed to sync leave and send notifications; usage and device data related to the Service; billing contact details (payment card data is processed by Stripe/Clerk, not stored in full by Recharge).

Categories of Data Subjects

Customer's employees, contractors, and other authorised users of the organisation workspace; invitees; and, where applicable, managers or admins who approve leave.

Schedule 2 - Sub-processors

Recharge uses the following Sub-processors. The live list at /security#subprocessors controls in case of conflict. Customer-enabled integrations process data only when Customer connects them.

Sub-processor | Purpose | Typical location

Clerk - Authentication, organisations, session management, and billing identity - USA / EEA (SCCs / adequacy as applicable)

Stripe - Payment processing (via Clerk Billing) - USA / EEA

Vercel - Application hosting, edge infrastructure, and AI Gateway - USA / EEA

Neon - Primary PostgreSQL datastore for Service data - European Union

Resend - Transactional email (invites, approvals, digests, notifications) - USA / EEA (SCCs / adequacy as applicable)

OpenAI (via Vercel AI Gateway) - Generation of leave suggestions from structured context - USA (SCCs / adequacy as applicable)

Customer-enabled integrations - Calendar sync and chat notifications Customer authorises (e.g. Google, Microsoft, Slack, Discord, Notion, webhooks) - Per integration provider

Schedule 3 - Technical and organisational measures (summary)

Further detail is published at /security. Measures may evolve; Recharge will not materially reduce the overall level of protection without notice where required by this DPA.

- Primary Service data hosted in the European Union (Neon PostgreSQL); application hosting on Vercel.
- Encryption in transit (TLS) and encryption at rest for Service data and integration credentials.
- Continuous database backups with point-in-time recovery via the database provider.
- Organisation-scoped access controls so one workspace cannot access another's records.
- Authentication and session management via Clerk; role-based access within organisations.
- OAuth for third-party integrations with least-privilege scopes; Customer can disconnect at any time.
- HMAC signing for outbound webhooks where applicable.
- Monitoring for uptime and performance; vulnerability reports accepted at support@recharge.app.
- AI suggestions use structured leave/coverage context rather than a full mirror of connected calendars.
- Data export available to organisation admins while the subscription is active; deletion on termination per clause 13 (typically within 30 days absent legal retention).

Schedule 4 - Signature

This DPA may be executed in counterparts (including electronic signature or acceptance via the Service). The parties' details for formal countersignature are:

Processor

[Processor legal name - Ltd, to be inserted] (trading as Recharge), company no. [Company number - to be inserted], registered office: [Registered office address - to be inserted]. Contact: support@recharge.app.

Customer

Legal name: _____
Company no. (if any): _____
Registered office: _____
Signatory name / title: _____
Email: _____
Signature / date: _____