Data Processing Agreement

CarbonBridge — pn v1.1, last reviewed 2026-04-23

Processor: [illegible] 91440300MA5G4UD231 · Legal rep h[illegible]ry) · legal@carbonbridge.com.cn

1. Parties

Controller — the customer entity identified in the service order ("Customer").

Processor — [illegible] Social Credit Code 91440300MA5G4UD231), trading as CarbonBridge ("CarbonBridge"), with legal representative h[illegible]ry).

2. Definitions

Capitalised terms carry the meaning given in the EU GDPR (Regulation 2016/679), the UK GDPR, and the PRC Personal Information Protection Law ("PIPL"). Where conflicts arise, the most protective regime applies to the affected data subject.

3. Scope & subject matter

CarbonBridge processes Customer data solely to provide CBAM compliance, carbon accounting, reporting, and related platform services.

Categories of data subjects: Customer employees, supply-chain contacts, and authorised partner staff who are invited to the platform.

Categories of data: identity (name, email, phone), organisational (company, role, USCC / EORI), transactional (calculations, emissions records, supplier exchanges), and operational logs (IP, user-agent, audit trail).

Sensitive categories are not processed. Customer must not upload special-category data (health, biometrics, politics, religion).

4. Processor obligations

Process Personal Data only on documented instructions from the Controller, including transfers to a third country, unless required by EU, UK, or PRC law (in which case CarbonBridge notifies the Controller before processing, unless prohibited).

Ensure personnel authorised to process Personal Data are bound by confidentiality.

Implement the technical and organisational measures in Schedule II (Security).

Not engage a sub-processor without the Controller's prior general written authorisation, which is given for the entities listed at https://www.carbonbridge.com.cn/trust-center/subprocessors. Material additions are announced e 14 days in advance and the Controller may object in writing.

Assist the Controller in responding to data-subject requests (access, rectification, erasure, portability) within 10 business days.

Assist the Controller with DPIAs and prior consultations under GDPR Art. 35–36.

Delete or return all Personal Data at the end of the service, except where retention is mandated by law (e.g. accounting records under PRC law — 10 years).

Make available all information necessary to demonstrate compliance; permit and contribute to audits, including on-site inspections with 30 days' notice (at the Controller's cost, once per year, under NDA).

5. International transfers

Personal Data originating in the EEA / UK is transferred to CarbonBridge under the European Commission's Standard Contractual Clauses (2021/914) Module 2 (Controller to Processor) — incorporated by reference.

Transfers from the PRC follow the PIPL Standard Contract for Cross-border Transfers of Personal Information (CAC, 2023) and require the Controller to complete the Personal Information Protection Impact Assessment before transfer.

6. Sub-processors

The current sub-processor list is maintained at https://www.carbonbridge.com.cn/trust-center/subprocessors and forms Schedule III of this DPA. CarbonBridge remains fully liable for its sub-processors' performance.

7. Security measures (Schedule II)

Encryption in transit (TLS 1.2+), encryption at rest for database backups, bcrypt-12 for passwords.

Role-based access control; principle of least privilege; unique authenticated accounts; MFA enforced for production administrators.

Network segmentation: application, database, and cache on a private bridge network; only Caddy reverse proxy is internet-facing on TCP/443.

Input validation with Zod schemas; CSRF double-submit; rate limiting; nonce-based Content-Security-Policy enforced.

Automated daily backups with monthly restore drills; 14-day retention; offsite relay copy is opt-in and enabled only when the shipping path is explicitly configured.

Structured JSON logging with 30-day retention on hot storage; Sentry error collection with PII scrubbing.

Quarterly dependency scans (npm audit, pip-audit), and a public disclosure channel at security@carbonbridge.com.cn.

Employee background checks before granting production access; access revoked within 24 hours of departure.

8. Breach notification

CarbonBridge notifies the Controller of a confirmed Personal Data breach without undue delay and in any event within 36 hours of confirmation.

The notification contains: nature of the breach, categories and approximate numbers of data subjects and records, likely consequences, and measures taken or proposed.

CarbonBridge cooperates with the Controller's own 72-hour notification duty to the supervisory authority under GDPR Art. 33.

For the PRC, breach notifications follow PIPL Art. 57 and the 2023 CAC Notice on Network Data Security Incident Reporting.

9. Audits

The Controller may audit CarbonBridge once per 12-month period, with 30 days' notice, during business hours, under NDA, and at its own cost. The audit covers compliance with this DPA. CarbonBridge may satisfy the audit obligation by providing a current SOC 2 or ISO 27001 attestation once available.

10. Liability & indemnity

Each party is liable for its own violations of applicable data-protection law. Aggregate liability under this DPA is capped at 12 months of fees paid by the Controller to CarbonBridge, except for breaches of confidentiality, IP, or indemnity obligations, which are uncapped.

11. Termination

This DPA terminates automatically with the main service agreement. CarbonBridge deletes Personal Data within 30 days of termination, except where retention is required by law, and certifies deletion on written request.

12. Governing law

For EEA/UK Controllers: Irish law, with courts of Dublin having jurisdiction (GDPR SCC Module 2). For PRC and other Controllers: PRC law, with Shenzhen International Arbitration Commission having jurisdiction under the SCIA Arbitration Rules.

Schedule I — Processing particulars

Processing duration: term of the service agreement + 30-day wind-down.

Nature and purpose: platform hosting, analytics, compliance reporting, CBAM filing support, AI-assisted drafting.

Frequency: continuous during service term.

Data subject categories: as in Section 3.

Data categories: as in Section 3.

Schedule II — Technical & organisational measures

As listed in Section 7.

Schedule III — Sub-processors

The live list is maintained at https://www.carbonbridge.com.cn/trust-center/subprocessors.