

DATA PROCESSING AGREEMENT

DPA — Version 1.0

CBAMCalc Platform · Ta-meri Systems

Party	Details
Data Processor	Ta-meri Systems — CBAMCalc Platform cbamcalc.company support@cbamcalc.company
Data Controller	[Customer Legal Name] [Registered Address] [Contact Email]
Effective Date	[Date of Signing]
Governing Law	European Union — GDPR (Regulation 2016/679)

Article 1 — Definitions

For the purposes of this Data Processing Agreement ("DPA"), the following terms shall have the meanings set out below:

- "Personal Data" means any information relating to an identified or identifiable natural person as defined in Article 4(1) GDPR.
- "Processing" means any operation performed on personal data, including collection, recording, storage, use, disclosure, or deletion.
- "Controller" means the Customer entity that determines the purposes and means of the processing of personal data.
- "Processor" means Ta-meri Systems, which processes personal data on behalf of the Controller.
- "Sub-processor" means any third party engaged by the Processor to process personal data on behalf of the Controller.
- "Supervisory Authority" means the competent data protection authority under applicable EU law.
- "Services" means the CBAMCalc platform and related services provided under the Master Subscription Agreement.

Article 2 — Subject Matter and Duration

2.1 This DPA governs the processing of personal data by Ta-meri Systems (Processor) on behalf of the Customer (Controller) in connection with the provision of the CBAMCalc Services.

2.2 This DPA shall remain in force for the duration of the Master Subscription Agreement and shall terminate automatically upon its expiry or termination, subject to Article 11 (Return and Deletion of Data).

Article 3 — Nature and Purpose of Processing

3.1 Categories of Personal Data Processed

Category	Examples	Purpose
Account data	Name, email, role, organization	Authentication & access control
Usage data	Login timestamps, IP addresses, actions	Audit logging, security, compliance
Business data	Import records, CN codes, emissions figures	CBAM calculation & reporting services
Communication data	Support emails, in-app messages	Customer support

3.2 Categories of Data Subjects

- Employees and authorized users of the Controller organization
- Supplier contacts where referenced in import records

3.3 Processing Activities

- Storage and retrieval of CBAM import and calculation records
- Authentication and session management
- Audit logging of user actions with timestamps and IP addresses
- Transmission to Sub-processors as listed in Article 8
- Generation of compliance reports and AI-powered insights

Article 4 — Obligations of the Processor

The Processor shall:

1. Process personal data only on documented instructions from the Controller, unless required by EU or Member State law.
2. Ensure that persons authorized to process personal data have committed to confidentiality.
3. Implement appropriate technical and organizational security measures in accordance with Article 5 of this DPA.
4. Respect the conditions for engaging Sub-processors as set out in Article 8.
5. Assist the Controller in ensuring compliance with data subject rights requests (Articles 15-22 GDPR) within 72 hours of receipt.
6. Assist the Controller in fulfilling its obligations under Articles 32-36 GDPR (security, breach notification, DPIA).
7. Delete or return all personal data upon termination of Services as per Article 11.
8. Make available all information necessary to demonstrate compliance with this DPA and allow for audits.

Article 5 — Security Measures

5.1 Technical Measures

Measure	Implementation	Status
Encryption at rest	AES-256 via Neon PostgreSQL managed encryption	✓ Active
Encryption in transit	TLS 1.2+ enforced on all connections	✓ Active
Access control	Role-based, organization-scoped, multi-tenant isolation	✓ Active
Multi-factor authentication	TOTP-based 2FA available for all accounts	✓ Active
Audit logging	All user actions logged with user, timestamp, IP, entity	✓ Active
Rate limiting	API rate limits on all endpoints including AI features	✓ Active
Security headers	CSP, HSTS, X-Frame-Options, X-Content-Type-Options	✓ Active
Penetration testing	Annual third-party assessment (scheduled)	🕒 Q3 2026

5.2 Organizational Measures

- Access to production systems limited to authorized personnel only
- Security awareness training for all staff with system access
- Vendor security assessments for all Sub-processors
- Incident response procedure documented and tested annually

Article 6 — Data Breach Notification

6.1 The Processor shall notify the Controller without undue delay — and no later than 48 hours after becoming aware — of any personal data breach affecting Controller data.

6.2 Notification shall include, to the extent available:

- Description of the nature of the breach including categories and approximate number of individuals affected
- Contact details of the Data Protection Officer or other contact point
- Likely consequences of the personal data breach
- Measures taken or proposed to address the breach

6.3 Notifications shall be sent to the Controller's designated contact email and to: security@cbamcalc.company

Article 7 — Data Subject Rights

The Processor shall assist the Controller in responding to requests from data subjects exercising their rights under GDPR Articles 15–22, including:

- Right of access (Art. 15) — export of all data held for a data subject
- Right to rectification (Art. 16) — correction of inaccurate personal data
- Right to erasure (Art. 17) — deletion of personal data upon verified request
- Right to data portability (Art. 20) — machine-readable export in JSON/CSV format
- Right to restrict processing (Art. 18) — account suspension without deletion

The Processor shall respond to forwarded data subject requests within 72 hours.

Article 8 — Sub-processors

8.1 The Controller hereby grants the Processor general authorization to engage Sub-processors, subject to the conditions of this Article.

8.2 Current Sub-processors (as of the Effective Date):

Sub-processor	Service	Data Location	Basis	DPA Link
Vercel Inc.	Application hosting & CDN	US / EU Edge	SCCs	vercel.com/legal/dpa
Neon Inc.	PostgreSQL database hosting	US-East (AWS)	SCCs	neon.tech/privacy
Anthropic PBC	AI analysis engine (CBAMCalc AI)	US	SCCs	anthropic.com/privacy
Paddle.com	Payment processing & subscriptions	UK / EU	SCCs / UK GDPR	paddle.com/legal/dpa
Resend Inc.	Transactional email delivery	US	SCCs	resend.com/legal
Sentry Inc.	Error monitoring & performance	US	SCCs	sentry.io/privacy

8.3 The Processor shall inform the Controller of any intended addition or replacement of Sub-processors at least 30 days in advance, giving the Controller the opportunity to object.

Article 9 — International Data Transfers

9.1 Where processing involves transfer of personal data to a third country, such transfer shall be subject to appropriate safeguards pursuant to GDPR Chapter V.

9.2 For transfers to Sub-processors in the United States, the Processor relies on Standard Contractual Clauses (SCCs) adopted by the European Commission (Decision 2021/914) as the legal mechanism for transfer.

9.3 The Controller may request copies of applicable SCCs from the Processor upon written request to: legal@cbamcalc.com

Article 10 — Audit Rights

10.1 The Processor shall make available all information necessary to demonstrate compliance with this DPA and shall allow for and contribute to audits and inspections conducted by the Controller or a mandated auditor.

10.2 Audits shall be conducted with at least 30 days written notice, during business hours, and no more than once per calendar year unless a security incident requires earlier inspection.

10.3 Audit costs shall be borne by the Controller unless deficiencies are identified, in which case costs shall be borne by the Processor.

Article 11 — Return and Deletion of Data

11.1 Upon termination or expiry of the Master Subscription Agreement, the Processor shall, at the Controller's choice:

- Return all personal data in machine-readable format (JSON/CSV) within 30 days of termination; or
- Securely delete all personal data and provide written confirmation of deletion within 30 days.

11.2 Audit logs shall be retained for 90 days post-termination for legal and compliance purposes before secure deletion.

11.3 Data portability features are available within the platform at: Settings → Data Export, enabling self-service export at any time during the subscription.

Article 12 — Liability

12.1 Each party shall be liable for damage caused by processing which infringes this DPA or GDPR. The Processor shall be exempt from liability if it can prove it is not in any way responsible for the event giving rise to damage.

12.2 Liability limitations set out in the Master Subscription Agreement shall apply to this DPA, except where GDPR mandates otherwise.

Article 13 — Signatures

For Ta-meri Systems (Processor)	For Customer (Controller)
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____
Signature: _____	Signature: _____