GRIDMARK

Data Processing Agreement

Gridmark Ltd — Standard Customer DPA

DATA PROCESSING AGREEMENT (DPA)

Last updated: 25 March 2026

This Data Processing Agreement ("DPA") is incorporated into and forms part of the Terms of Service or subscription agreement (the "Principal Agreement") between the entity agreeing to these terms ("Controller" or "Customer") and Gridmark Ltd, Company No. 17087910, 71-75 Shelton Street, London WC2H 9JQ ("Processor" or "Gridmark"), pursuant to which Processor provides the SiteChip equipment tracking and compliance recording platform (the "Services") to Controller.

By using the Services, Controller agrees to be bound by this DPA. If Controller does not agree to this DPA, Controller must not use the Services.

This DPA sets forth the terms and conditions under which Processor will process Personal Data on behalf of Controller in accordance with UK GDPR Article 28 and other applicable Data Protection Laws.

1. DEFINITIONS

1.1

The following terms have the meanings set forth below:

(a) **"Controller"** means the entity that determines the purposes and means of processing Personal Data. In this DPA, Controller is the Customer.

(b) **"Processor"** means the entity that processes Personal Data on behalf of the Controller. In this DPA, Processor is Gridmark Ltd.

(c) **"Sub-processor"** means any third-party processor engaged by the Processor to process Personal Data on behalf of the Controller.

(d) **"Personal Data"** means any information relating to an identified or identifiable natural person as defined in Article 4(1) of the UK GDPR and applicable Data Protection Laws.

(e) **"Processing"** means any operation or set of operations performed on Personal Data, such as collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, erasure, or destruction, as defined in Article 4(2) of the UK GDPR.

(f) **"Data Subject"** means an identified or identifiable natural person to whom Personal Data relates.

(g) **"Data Protection Laws"** means all applicable laws and regulations relating to data protection and privacy, including but not limited to: the UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018, the General Data Protection Regulation (EU) 2016/679 ("GDPR") where applicable, the EU ePrivacy Directive (Directive 2002/58/EC), and the Privacy and Electronic Communications Regulations 2003.

(h) **"Supervisory Authority"** means the UK Information Commissioner's Office (ICO) or any other independent public authority established by an EU Member State or the UK pursuant to the GDPR or UK GDPR.

(i) **"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise

processed, as defined in Article 4(12) of the UK GDPR.

(j) **"Standard Contractual Clauses" or "SCCs"** means the standard contractual clauses for the transfer of Personal Data to third countries approved by the European Commission pursuant to GDPR Article 46(2)(c), as may be updated from time to time.

(k) **"UK IDTA"** means the UK International Data Transfer Agreement issued by the UK Information Commissioner's Office (ICO) pursuant to Section 119A of the Data Protection Act 2018.

(l) **"Restricted Transfer"** means a transfer of Personal Data from the European Economic Area ("EEA") or the United Kingdom ("UK") to a country that has not been recognised by the European Commission or UK government as providing an adequate level of data protection.

1.2

Capitalised terms not defined in this DPA have the meanings set forth in the Principal Agreement or the UK GDPR.

2. SCOPE AND DURATION OF PROCESSING

2.1 Subject Matter and Duration

This DPA applies to the Processing of Personal Data by Processor on behalf of Controller in connection with the provision of the Services under the Principal Agreement.

Duration of Processing: The Processing will continue for the duration of the Principal Agreement, unless otherwise terminated in accordance with the terms of this DPA or the Principal Agreement.

2.2 Nature and Purpose of Processing

The Processor shall process Personal Data on behalf of the Controller for the following purposes:

- To provide the SiteChip NFC-based equipment tracking and compliance recording platform as described in the Principal Agreement
- To record equipment check-out and return events initiated by workers via NFC tag interactions
- To record compliance check events including photographic evidence of equipment inspections
- To authenticate workers via WebAuthn passkeys for identity verification
- To generate compliance reports and export records for the Controller

2.3 Types of Personal Data

The Personal Data processed under this DPA is limited to:

- **Worker first names** — used for identification on check events and compliance records. No surnames are collected.
- **Timestamps** — server-generated date and time of each interaction.
- **Device information** — device model name recorded during compliance photo capture.

- **Compliance photographs** — images of equipment taken during compliance checks, with metadata overlay (worker first name, timestamp, device model).
- **WebAuthn credential identifiers** — cryptographic public key identifiers stored for passkey authentication. No biometric data is collected or stored by the Processor.

2.4 Categories of Data Subjects

The Data Subjects whose Personal Data may be processed include:

- Workers and staff of the Controller who interact with NFC tags at the Controller's premises.

2.5 Special Categories of Data

This DPA does not authorise Processor to process special categories of Personal Data as defined in Article 9 of the UK GDPR. No such data is collected by the Services.

3. OBLIGATIONS OF THE PROCESSOR

3.1 Processing Instructions

(a) Processor shall process Personal Data only on documented instructions from the Controller, unless required to do so by EU, Member State, or UK law to which the Processor is subject. In such cases, the Processor shall inform the Controller of that legal requirement before processing, unless the law prohibits such information on important grounds of public interest.

(b) The initial instructions for Processing are set forth in this DPA and the Principal Agreement. Any additional or alternative instructions must be agreed upon in writing by both Parties.

(c) If Processor believes that any instruction from Controller violates the UK GDPR or other Data Protection Laws, Processor shall immediately inform Controller.

3.2 Confidentiality

(a) Processor shall ensure that all persons authorised to process Personal Data on behalf of Controller (including Processor's employees, contractors, and agents) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(b) Processor shall maintain the confidentiality of all Personal Data and shall not disclose Personal Data to any third party except as permitted under this DPA or as required by law.

3.3 Security of Processing (Article 32 UK GDPR)

(a) Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of Processing, taking into account: the state of the art; the costs of implementation; the nature, scope, context, and purposes of Processing; and the risk of varying likelihood and severity for the rights and freedoms of natural persons.

(b) Such measures shall include, as appropriate:

- (i) Encryption of Personal Data in transit and at rest;
- (ii) Ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
- (iii) Ability to restore availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
- (iv) Regular testing, assessment, and evaluation of the effectiveness of technical and organisational measures;
- (v) Access controls (including multi-factor authentication and role-based access control) to ensure that only authorised personnel can access Personal Data;
- (vi) Data minimisation (Processing only the minimum Personal Data necessary for the purposes);
- (vii) Secure data deletion (ensuring Personal Data is securely deleted when no longer needed);
- (viii) Incident response plan (procedures for detecting, reporting, and responding to Personal Data Breaches);
- (ix) Network security (firewalls, secure transmission protocols).

(c) Processor shall conduct regular security assessments to ensure the effectiveness of security measures and shall promptly remediate any identified vulnerabilities.

(d) **Detailed Security Measures:** A comprehensive description of Processor's technical and organisational security measures is set forth in Annex 2 (Security Measures) to this DPA.

3.4 Sub-processors

(a) **General Authorisation:** Controller provides general written authorisation for Processor to engage Sub-processors, subject to the conditions set forth in this Section 3.4.

(b) **Current Sub-processors:** Processor currently engages the Sub-processors listed in Annex 3 (Sub-processors) to this DPA.

(c) **Notification and Objection:** Processor shall inform Controller of any intended changes concerning the addition or replacement of Sub-processors at least 30 days in advance ("Notification Period"). Controller may object to the engagement of a new Sub-processor on reasonable grounds relating to data protection within 14 days of receiving notice ("Objection Period"). If Controller objects, the Parties shall work together in good faith to find a commercially reasonable solution. If no solution is found within 30 days, either Party may terminate the Principal Agreement with respect to the Services that require the use of the objected Sub-processor, without penalty.

(d) **Sub-processor Agreements:** Where Processor engages a Sub-processor for carrying out specific Processing activities on behalf of Controller:

- (i) Processor shall enter into a written agreement with the Sub-processor that imposes data protection obligations equivalent to those set forth in this DPA, including appropriate technical and organisational measures.
- (ii) Processor shall ensure that the Sub-processor complies with the UK GDPR and other applicable Data Protection Laws.

- (iii) Processor remains fully liable to Controller for the performance of the Sub-processor's obligations under the Sub-processor agreement and for any failure by the Sub-processor to fulfil its data protection obligations.

(e) **Sub-processor Audits:** Controller has the right to audit Sub-processors (or appoint an independent auditor to audit Sub-processors) to verify compliance with the Sub-processor's data protection obligations, subject to the same terms as set forth in Section 3.8 (Audit and Inspection Rights).

3.5 Assistance with Data Subject Rights (Chapter III UK GDPR)

(a) Processor shall assist Controller in responding to requests from Data Subjects to exercise their rights under the UK GDPR or other Data Protection Laws, including: right of access (Article 15); right to rectification (Article 16); right to erasure (Article 17); right to restriction of processing (Article 18); right to data portability (Article 20); right to object (Article 21); and rights related to automated decision-making and profiling (Article 22).

(b) Processor shall provide reasonable assistance to Controller in responding to Data Subject requests within 14 days of receiving Controller's request for assistance, or within such shorter timeframe as may be required by Data Protection Laws.

(c) If Processor receives a Data Subject request directly, Processor shall promptly forward the request to Controller (within 2 business days) and shall not respond to the request without Controller's prior written authorisation, unless required by law.

3.6 Assistance with Controller's Compliance Obligations

(a) Processor shall assist Controller in ensuring compliance with the obligations pursuant to:

- (i) Article 32 UK GDPR (Security of Processing) — by implementing and maintaining appropriate technical and organisational measures as described in Section 3.3 and Annex 2.
- (ii) Articles 33-34 UK GDPR (Personal Data Breach Notification) — by notifying Controller of Personal Data Breaches as described in Section 3.7.
- (iii) Articles 35-36 UK GDPR (Data Protection Impact Assessment and Prior Consultation) — by providing information reasonably necessary for Controller to conduct a DPIA or consult with a Supervisory Authority, if required.

(b) Processor shall provide Controller with all information reasonably necessary to demonstrate compliance with the obligations set forth in this DPA and the UK GDPR.

3.7 Personal Data Breach Notification

(a) Processor shall notify Controller without undue delay and, where feasible, within 72 hours of becoming aware of a Personal Data Breach.

(b) The notification shall include, to the extent available:

- (i) A description of the nature of the Personal Data Breach, including the categories and approximate number of Data Subjects and Personal Data records affected;
- (ii) The name and contact details of Processor's privacy contact;
- (iii) A description of the likely consequences of the Personal Data Breach;

- (iv) A description of the measures taken or proposed to be taken by Processor to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

(c) Processor shall provide reasonable assistance to Controller in: notifying the Supervisory Authority of the Personal Data Breach (if required by Article 33 UK GDPR); notifying affected Data Subjects of the Personal Data Breach (if required by Article 34 UK GDPR); and investigating, mitigating, and remediating the Personal Data Breach.

(d) Processor shall not notify any third party (including Data Subjects, Supervisory Authorities, or the media) of a Personal Data Breach without Controller's prior written consent, except as required by law.

(e) Processor shall document all Personal Data Breaches and maintain records for at least 5 years, or as required by Data Protection Laws.

3.8 Audit and Inspection Rights

(a) Processor shall allow Controller (or Controller's appointed independent auditor) to conduct audits and inspections to verify Processor's compliance with this DPA and applicable Data Protection Laws.

(b) **Audit Frequency:** Controller may conduct audits once per year upon reasonable notice, or more frequently if: (i) required by a Supervisory Authority; (ii) a Personal Data Breach has occurred; or (iii) Controller has reasonable grounds to believe Processor is not complying with this DPA.

(c) **Audit Notice:** Controller shall provide Processor with at least 30 days' prior written notice of an audit, except in the case of a Personal Data Breach or Supervisory Authority request, in which case shorter notice (or no notice) may be provided.

(d) **Audit Scope:** Audits may include: (i) review of Processor's technical and organisational security measures; (ii) review of Processor's policies, procedures, and documentation related to data protection; (iii) interviews with Processor's personnel; (iv) inspection of Processor's facilities and systems (subject to reasonable security and confidentiality restrictions).

(e) **Audit Reports:** Processor may satisfy the audit requirement by providing Controller with a copy of a recent third-party audit report (e.g., Cyber Essentials certification, SOC 2 Type II) if such report adequately demonstrates compliance with this DPA.

(f) **Audit Costs:** Controller shall bear the costs of the audit, unless the audit reveals a material breach of this DPA by Processor, in which case Processor shall reimburse Controller for reasonable audit costs.

(g) **Confidentiality:** Controller and its auditors shall maintain the confidentiality of any information obtained during the audit and shall use such information solely for the purpose of verifying compliance with this DPA.

3.9 Deletion or Return of Personal Data

(a) Upon termination of the Principal Agreement or upon Controller's written request, Processor shall, at Controller's choice: (i) delete all Personal Data in Processor's possession or control; or (ii) return all Personal Data to Controller in a commonly used, machine-readable format.

(b) **Deletion Timeframe:** Processor shall delete or return Personal Data within 30 days of termination or request, unless otherwise agreed in writing.

(c) **Secure Deletion:** Processor shall delete Personal Data using secure methods to ensure the data cannot be recovered.

(d) **Retention Exceptions:** Processor may retain Personal Data to the extent required by UK law, provided that Processor: (i) informs Controller of the legal requirement to retain Personal Data; (ii) continues to protect the confidentiality and security of the retained Personal Data; and (iii) processes the retained Personal Data solely for the purpose required by law.

(e) **Certification of Deletion:** Upon Controller's request, Processor shall provide written certification that all Personal Data has been deleted or returned, and that no copies remain in Processor's systems (except as permitted under Section 3.9(d)).

(f) **Backup Retention:** Personal Data may remain in Processor's backup systems for up to 30 days after deletion, provided that such backup data is not accessible for normal operations and will be securely deleted in accordance with Processor's backup retention schedule.

4. INTERNATIONAL DATA TRANSFERS

4.1 Processor's primary data processing infrastructure is located in the EU (London, United Kingdom). Personal Data is not routinely transferred outside the United Kingdom or the European Economic Area.

4.2 Processor's Sub-processors (listed in Annex 3) are US-headquartered companies. Data processing for the Services is configured to use EU/UK data centres. Where any processing occurs in the United States, transfers are protected by Standard Contractual Clauses or the UK International Data Transfer Agreement as applicable, and by the sub-processors' compliance with recognised data privacy frameworks.

4.3 If any future Restricted Transfer of Personal Data is required, Processor shall implement appropriate safeguards in accordance with Chapter V of the UK GDPR before any such transfer takes place, including execution of the UK IDTA or EU SCCs as applicable, and shall notify Controller in advance.

4.4 Processor shall continuously monitor the legal and factual circumstances surrounding international data transfers and shall immediately notify Controller if: (i) Processor is no longer able to comply with the transfer mechanisms in place; (ii) Processor receives a request from a government authority or court to disclose Personal Data (subject to legal restrictions on such notification); or (iii) there are changes to the laws or practices of a destination country that may affect the adequacy of protection for Personal Data.

5. LIABILITY AND INDEMNIFICATION

5.1 **Liability Under UK GDPR:** Each Party shall be liable for damage caused by its Processing of Personal Data to the extent such Processing is in violation of the UK GDPR or this DPA, in accordance with Articles 82-83 of the UK GDPR.

5.2 **Indemnification by Processor:** Processor shall indemnify, defend, and hold harmless Controller from and against any and all losses, damages, liabilities, costs, and expenses (including reasonable legal fees) arising out of or relating to: (a) Processor's breach of this DPA or applicable Data Protection Laws; (b) Processor's failure to implement appropriate technical and organisational security measures; (c) any Personal Data Breach caused by Processor's negligence or wilful misconduct; (d) third-party claims (including Data Subject claims and Supervisory Authority fines or penalties) arising from Processor's non-compliance with this DPA or Data Protection Laws.

5.3 **Limitation of Liability:** Notwithstanding any limitation of liability in the Principal Agreement, Processor's liability for violations of this DPA or Data Protection Laws shall not be limited or excluded, except to the extent such limitation or exclusion is expressly permitted by applicable law.

6. TERM AND TERMINATION

6.1 **Term:** This DPA shall commence on the date Controller first uses the Services and shall remain in effect for the duration of the Principal Agreement, unless earlier terminated in accordance with this Section 6.

6.2 **Termination:** (a) Either Party may terminate this DPA if the other Party materially breaches this DPA and fails to cure such breach within 30 days of receiving written notice. (b) Controller may terminate this DPA (and the Principal Agreement) immediately if: (i) Processor is unable to comply with this DPA or Data Protection Laws; (ii) Processor suffers a significant Personal Data Breach that compromises the security or confidentiality of Personal Data; (iii) a Supervisory Authority orders Controller to cease using Processor's services due to non-compliance.

6.3 Upon termination of this DPA or the Principal Agreement, Processor shall delete or return Personal Data as described in Section 3.9.

6.4 **Survival:** The following provisions shall survive termination of this DPA: Sections 3.2 (Confidentiality), 3.9 (Deletion or Return of Personal Data), 5 (Liability and Indemnification), 6.4 (Survival), and 7 (General Provisions).

7. GENERAL PROVISIONS

7.1 **Relationship to Principal Agreement:** This DPA is incorporated into and forms part of the Principal Agreement. In the event of a conflict between this DPA and the Principal Agreement with respect to data protection matters, this DPA shall prevail.

7.2 **Amendments:** This DPA may be amended by Processor. For minor administrative changes, the Processor will publish an updated version on its website. For material changes that affect the Controller's rights or obligations, the Processor will notify the Controller by email at least 30 days before the changes take effect. If the Controller does not agree to the material changes, the Controller may terminate the Principal Agreement before the changes take effect without penalty. Continued use of the Services after the 30-day notice period constitutes acceptance of the amended DPA.

7.3 **Severability:** If any provision of this DPA is held to be invalid, illegal, or unenforceable, the remaining provisions shall remain in full force and effect. The Parties shall negotiate in good faith to replace any invalid provision with a valid provision that achieves, to the extent possible, the original intent.

7.4 **Governing Law:** This DPA shall be governed by and construed in accordance with the laws of England and Wales.

7.5 **Jurisdiction:** Any dispute arising out of or relating to this DPA shall be subject to the exclusive jurisdiction of the courts of England and Wales, except that Data Subjects shall retain the right to bring claims in the courts of the country where they have their habitual residence, in accordance with Article 79 of the UK GDPR.

7.6 **Order of Precedence:** In the event of a conflict between: (a) this DPA and the Principal Agreement — this DPA prevails with respect to data protection matters; (b) this DPA and the Standard Contractual Clauses or UK IDTA — the SCCs/UK IDTA prevail.

7.7 **Entire Agreement:** This DPA, together with the Principal Agreement and all annexes, constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes all prior or contemporaneous agreements, understandings, or representations, whether written or oral.

7.8 **Notices:** All notices under this DPA shall be in writing and delivered to the contact addresses provided in the Principal Agreement, or to support@sitechip.co.uk for notices to the Processor.

7.9 **Language:** This DPA is executed in English.

ANNEX 1: DETAILS OF PROCESSING

Nature of Processing	Processor will store, retrieve, and process Personal Data in connection with providing the Site
Purpose of Processing	To enable Controller to track equipment custody, record compliance checks with photographi
Duration of Processing	For the term of the Principal Agreement, plus 30 days for data deletion or return.
Types of Personal Data	Worker first names, server-generated timestamps, device model, compliance photographs wi
Categories of Data Subjects	Workers and staff of the Controller who interact with NFC tags at Controller's premises.
Special Categories of Data	None. This DPA does not authorise processing of special categories of Personal Data as defi
Processing Location	EU (London, United Kingdom). Sub-processor infrastructure configured for EU/UK data centre

ANNEX 2: TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

A. Infrastructure Security

- All data transmitted over HTTPS using TLS 1.2 or higher. No unencrypted connections permitted.
- Database hosted on Supabase (SOC 2 Type II certified) with encryption at rest.
- Website and CDN provided by Cloudflare with DDoS protection and edge caching.
- All infrastructure configured to process data in EU (London) data centres.

B. Authentication and Access Control

- Worker identity verified via WebAuthn passkeys (Face ID / fingerprint). Biometric data never leaves the worker's device and is never transmitted to or stored by the Processor.
- Workers must be approved by a manager before accessing any functionality.
- Dashboard access protected by PIN/password authentication.
- Multi-factor authentication enabled on all administrative accounts (database, hosting, source code, email).
- Row-level security policies on the database ensure data isolation between sites.
- Declined workers are blocked from re-registration.

C. Data Minimisation

- Only worker first names are collected. No surnames, email addresses, phone numbers, or home addresses.
- No GPS or location data is collected or stored.
- Compliance photographs are camera-only capture (gallery uploads blocked) to ensure authenticity.
- Server-side timestamps are used for all events. Client-side times cannot be altered.

D. Backup and Recovery

- Automated daily database backups with point-in-time recovery capability.
- Backups encrypted and stored separately from primary database infrastructure.
- Backup retention in accordance with infrastructure provider's standard retention policy.

E. Incident Response

- Documented incident response procedures.
- Breach notification to Controller within 72 hours of becoming aware of a Personal Data Breach.
- Post-incident review and remediation for all security events.
- Breach records maintained for a minimum of 5 years.

F. Certifications

• **ICO Registration:** Gridmark Ltd is registered with the UK Information Commissioner's Office (Ref: ZC109151).

• **Cyber Essentials:** UK government-backed cybersecurity certification. Certificate: ffc8402c-96dd-4b89-895a-b46be21dfc3b. Certified 25 March 2026.

• **Infrastructure:** Supabase Inc maintains SOC 2 Type II certification, independently audited annually. Cloudflare Inc maintains comprehensive security certifications.

ANNEX 3: LIST OF SUB-PROCESSORS

Sub-processor	Service Provided	Processing Location	Data Processed
Supabase Inc	Database, authentication, file storage	EU (London)	All Personal Data types listed in Section 2.3
Cloudflare Inc	Website hosting, CDN, DDoS protection	EU	Web traffic data (IP addresses, request headers) processed transiently
Stripe Payments Europe Ltd	Payment processing and subscription billing	EU (Ireland)	Customer names, email addresses, payment card details, transaction data

Sub-processor Change Notification

Processor shall notify Controller of any changes to this list at least 30 days in advance by email to the contact address provided in the Principal Agreement. Controller may object within 14 days of receiving notice. If no resolution is reached within 30 days, Controller may terminate the Principal Agreement with respect to the Services requiring the objected Sub-processor.

Supabase Inc, Cloudflare Inc, and Stripe Payments Europe Ltd each maintain signed Data Processing Agreements with Gridmark Ltd. Copies are available on request.