TRIDENT HR

Data Processing Agreement

Made under Article 28 of the UK GDPR

Trident HR Ltd · Registered in Scotland SC864348
3 Newton Place, Glasgow, G3 7PR

Version 2.0 · July 2026

This Data Processing Agreement (the "Agreement") forms part of, and is subject to, the agreement between the Client and Trident HR Ltd under which Trident HR Ltd provides the Trident Command platform and/or HR consultancy services — being the Trident Command Subscription Terms and/or the HR Consultancy Services Agreement, as applicable (together or individually, the "Principal Agreement"). It sets out the terms on which Trident HR Ltd processes personal data on behalf of the Client.

Parties

Role	Details
The Processor	Trident HR Ltd · Company number SC864348 · 3 Newton Place, Glasgow, G3 7PR · ICO registration ZC074452 · admin@tridenthr.co.uk
The Controller	The client organisation receiving services under the Principal Agreement ("the Client"), as identified in the Principal Agreement, Engagement Details or applicable order.

Each a "Party" and together the "Parties".

1. Definitions and Interpretation

1.1 "Data Protection Legislation" means the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003, and all other applicable laws relating to the processing of personal data and privacy, as amended or replaced from time to time, including by the Data (Use and Access) Act 2025. "UK GDPR" has the meaning given in section 3(10) of the Data Protection Act 2018. "Controller", "Processor", "Data Subject", "Personal Data", "Personal Data Breach", "Processing" and "Special Category Data" have the meanings given in the Data Protection Legislation. "Client Personal Data" means any Personal Data the Processor processes on behalf of the Controller under or in connection with the Principal Agreement, as described in Schedule 1. "Sub-processor" means any third party engaged by the Processor to process Client Personal Data. Capitalised terms not defined here have the meaning given in the Principal Agreement.

1.2 This Agreement is in addition to, and does not relieve, remove or replace, a Party's obligations under the Data Protection Legislation. In the event of any conflict between this Agreement and the Principal Agreement on the subject of data protection, this Agreement prevails.

2. Roles of the Parties

2.1 For the purposes of the Data Protection Legislation, the Controller is the data controller and the Processor is the data processor in respect of the Client Personal Data.

2.2 The Controller determines the purposes and means of the processing of Client Personal Data and is responsible for ensuring it has a valid lawful basis under Article 6 of the UK GDPR and, where applicable, a condition for processing Special Category Data under Article 9, for all processing carried out under this Agreement.

2.3 The Processor processes Client Personal Data only on behalf of the Controller and in accordance with this Agreement and the Controller's documented instructions.

3. Processor Obligations

The Processor shall, in respect of all Client Personal Data:

3.1 Documented instructions. Process the Client Personal Data only on the documented instructions of the Controller, including with regard to transfers of Client Personal Data to a third country, unless required to do otherwise by applicable law. Where the Processor is required by law to process Client Personal Data other than on the Controller's instructions, it shall inform the Controller of that legal requirement before processing, unless the law prohibits such disclosure on important grounds of public interest. The Principal Agreement, this Agreement and the configuration choices made by the Controller within the Platform together constitute the Controller's documented instructions.

3.2 Duty of confidentiality. Ensure that all persons authorised to process the Client Personal Data are bound by an appropriate obligation of confidentiality, whether contractual or statutory.

3.3 Security of processing. Take all measures required pursuant to Article 32 of the UK GDPR, implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The measures in place are described in Schedule 3.

3.4 Sub-processors. Not engage a Sub-processor without the prior general written authorisation of the Controller. The Controller provides general authorisation for the Processor to engage the Sub-processors listed in Schedule 2. The Processor shall inform the Controller of any intended addition or replacement of Sub-processors, giving the Controller a reasonable opportunity to object. Where the Processor engages a Sub-processor, it shall put in place a written contract imposing data protection obligations equivalent to those set out in this Agreement, and remains fully liable to the Controller for the performance of that Sub-processor's obligations.

3.5 Assistance with data subject rights. Taking into account the nature of the processing, assist the Controller by appropriate technical and organisational measures, insofar as is possible, in fulfilling the Controller's obligation to respond to requests from Data Subjects exercising their rights under Chapter III of the UK GDPR. The Platform provides functionality enabling the Controller to access, rectify, export and delete Client Personal Data.

3.6 Assistance with controller obligations. Taking into account the nature of processing and the information available to the Processor, assist the Controller in ensuring compliance with its obligations under Articles 32 to 36 of the UK GDPR, including security of processing, notification of Personal Data Breaches, communication of breaches to Data Subjects, data protection impact assessments, and prior consultation with the Information Commissioner's Office.

3.7 Personal data breaches. Notify the Controller without undue delay, and in any event within 48 hours, after becoming aware of a Personal Data Breach affecting Client Personal Data. Such notification shall describe, to the extent known, 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 it. The Processor shall provide reasonable cooperation to assist the Controller in meeting its own breach-notification obligations.

3.8 Deletion or return of data. At the choice of the Controller, delete or return all Client Personal Data to the Controller after the end of the provision of services relating to processing, and delete existing copies unless applicable law requires storage of the Client Personal Data. The Processor shall, on request, certify completion of such deletion.

3.9 Audits and inspections. Make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the UK GDPR,

and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller. Such audits shall be conducted on reasonable prior written notice, during normal business hours, no more than once per year (save where required by a supervisory authority or following a Personal Data Breach), and subject to appropriate confidentiality obligations. The Processor may satisfy this obligation by providing relevant certifications or third-party audit reports where available.

3.10 Duty to inform. Immediately inform the Controller if, in the Processor's opinion, an instruction given by the Controller infringes the Data Protection Legislation.

4. Controller Obligations

4.1 The Controller warrants that it has, and will maintain throughout the term, a valid lawful basis under Article 6 of the UK GDPR for the processing of Client Personal Data, and where Special Category Data (including health, sickness and absence information) is processed, a valid condition under Article 9 of the UK GDPR together with any associated condition under Schedule 1 of the Data Protection Act 2018.

4.2 Where the Controller relies on the condition in Article 9(2)(b) (employment, social security and social protection), or any other condition requiring it, the Controller warrants that it maintains an appropriate policy document as required by Schedule 1 of the Data Protection Act 2018.

4.3 The Controller is responsible for ensuring that its instructions to the Processor, including its configuration and use of the Platform, comply with the Data Protection Legislation, and that it has provided all necessary privacy information to, and obtained any necessary consents from, the relevant Data Subjects.

5. International Transfers

5.1 The Processor shall not transfer Client Personal Data to a country outside the United Kingdom unless it has taken such measures as are necessary to ensure the transfer complies with the Data Protection Legislation. Such measures may include transferring only to a country subject to UK adequacy regulations, or pursuant to an appropriate safeguard such as the International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses.

5.2 The primary hosting of Client Personal Data takes place within the United Kingdom and the European Economic Area, as set out in Schedule 2.

6. Liability, Term and General

6.1 The liability of each Party under or in connection with this Agreement is subject to the limitations and exclusions of liability set out in the Principal Agreement.

6.2 This Agreement takes effect on the commencement date of the Principal Agreement and continues for so long as the Processor processes Client Personal Data on behalf of the Controller.

6.3 This Agreement is governed by the laws of Scotland, and the Parties submit to the exclusive jurisdiction of the Scottish courts, save that either Party may seek interim relief in any court of competent jurisdiction.

6.4 If any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions continue in full force and effect.

Signatures

The Processor — for and on behalf of Trident HR Ltd

Name: _____

Title: _____

Signature: _____

Date: _____

The Controller — for and on behalf of the Client

Name: _____

Title: _____

Company: _____

Signature: _____

Date: _____

Schedule 1 — Details of Processing

Item	Description
Subject matter	The provision of the Trident Command platform and associated services, and (where engaged) HR consultancy services including HR case management, documentation and records, as described in the Principal Agreement.
Duration	The term of the Principal Agreement, and any subsequent period during which the Processor processes Client Personal Data on the Controller's behalf.
Nature and purpose	Hosting, storage, organisation, retrieval, display and transmission of workforce personal data to enable the Controller to manage its human resources, attendance, absence, performance, HR casework and related functions.
Categories of Data Subjects	Employees of the Controller; workers, contractors and agency staff of the Controller; managers and administrators of the Controller; emergency contacts nominated by the above.
Types of Personal Data	Identity and contact data (name, work email, work phone, job title, department, profile photograph); personal contact data where held (personal phone, personal email, home address, date of birth); emergency contact details; attendance and working-time data (clock-in/out records, timecards, flexi, rotas); holiday entitlement and requests; performance data (reviews, goals, one-to-one records); HR case records (disciplinary, grievance, absence and related casework, where consultancy services are engaged); documents and acknowledgements; wellbeing check-ins; precise location data captured at the point of clocking in or out; support requests and correspondence; account identifiers and technical/usage data.
Special Category Data	Data concerning health, namely sickness and absence records, fit notes, and related information. Processed only where the Controller has enabled the relevant functionality and has established an appropriate Article 9 condition and, where required, an appropriate policy document.

Schedule 2 — Authorised Sub-processors

The Controller authorises the Processor to engage the following Sub-processors. The Processor will give notice of any intended addition or replacement, providing a reasonable opportunity to object.

Sub-processor	Service provided	Location	Processing activity
Supabase, Inc.	Database, authentication and file storage	European Union (Ireland)	Hosting of all Platform data
Vercel, Inc.	Application hosting	European Union / United Kingdom	Hosting of web application
Microsoft Corporation	Email, calendar and single sign-on	European Union / United Kingdom	Transactional email, calendar integration, SSO
Stripe, Inc.	Payment processing and billing	United States (with appropriate safeguards)	Billing administration and payment collection
Anthropic, PBC	AI content generation	United States (with appropriate safeguards)	Processing of content submitted to the Platform's AI-assisted document and course features, solely to return results
Resend, Inc.	Transactional email delivery	United States (with appropriate safeguards)	Delivery of system emails
Apple Inc. (APNs)	Push notification delivery	United States (with appropriate safeguards)	Mobile push notifications (iOS)
Google LLC (FCM)	Push notification delivery	United States (with appropriate safeguards)	Mobile push notifications (Android)
Expo (650 Industries, Inc.)	Push notification tooling	United States (with appropriate safeguards)	Mobile push notification dispatch

The current list of Sub-processors is maintained by the Processor and may be updated in accordance with clause 3.4 of this Agreement.

Schedule 3 — Technical and Organisational Security Measures

The Processor implements and maintains the following measures to protect Client Personal Data, in accordance with Article 32 of the UK GDPR:

Access control

- Role-based access controls restricting access to Client Personal Data to authorised users on a least-privilege basis.
- Logical isolation (multi-tenancy separation) between client organisations, enforced at the database level.
- Authentication via Microsoft 365 single sign-on or password-based sign-in, with optional biometric app lock on mobile devices.
- Enforcement of password and session controls.

Encryption

- Encryption of Client Personal Data in transit using industry-standard transport layer security.
- Encryption of Client Personal Data at rest.
- Encryption of integration credentials and tokens using strong cryptographic methods.

Operational security

- Audit logging of access to and changes within the Platform.
- Regular application and dependency updates.
- Hosting with reputable infrastructure providers offering high availability and resilience.
- Backup and recovery procedures enabling restoration of Client Personal Data in the event of an incident.

Organisational measures

- Cyber Essentials certification held by the Processor.
- Confidentiality obligations imposed on all personnel with access to Client Personal Data.
- Sub-processors bound by written contracts imposing equivalent data protection obligations.
- Personal Data Breach notification procedures consistent with clause 3.7.