timeware®
HR, Time and Attendance Software

CLOUD SOFTWARE

Updated 6 May 2026

timeware® Cloud Security & Infrastructure Briefing for IT Departments

At timeware UK Ltd, we prioritise security, compliance, and data integrity in our cloud-based HR and time and attendance solution. This briefing outlines the technical architecture and controls to address any IT concerns.

Ensures robust data handling compliance aligned with GDPR and other relevant regulations.

1. UK Data Sovereignty

- All customer data is stored in the UK.
- Primary hosting region: UK South (London); disaster recovery region: UK West (Cardiff).
- Every Azure service (SQL, Blob Storage, Service Bus, etc.) is deployed exclusively in UK regions, ensuring compliance with UK GDPR and the Data Protection Act 2018.

2. Built on Microsoft Azure

- AES-256 Transparent Data Encryption (TDE) on all Azure SQL databases.
- Geo-redundant Blob Storage and active geo-replication from UK South to UK West.
- Azure Front Door Premium with Web Application Firewall (WAF) and DDoS protection.
- TLS 1.2 minimum for data in transit.
- Managed Identity prevents stored credentials between services.
- 35-day point-in-time restore plus weekly, monthly, and yearly backups.
- Microsoft Defender for SQL and Storage for threat detection and malware scanning.

3. Security Enhancements by timeware®

- Single Sign-On via Microsoft Entra ID, with optional OIDC support.
- Multi-factor authentication (TOTP, SMS, recovery codes), configurable per tenant.
- Account lockout thresholds and password policies (length, complexity, banned words).
- SHA-256 hashed API keys and HMAC-SHA256 webhook signing.
- Anti-forgery (CSRF) protection and hardened session cookies.
- Fine-grained API permission-gating and JWT validation with RSA key rotation.

CYBER ESSENTIALS PLUS

Citation ISO Certification
Integrated Management System
ISO 9001: 2015
ISO 27001: 2022
REGISTERED
Certificate No: 491342025

Company Name: timeware (UK) Ltd.
Registered Office: 3 Fieldhouse Road, Rochdale, Greater Manchester, OL12 0AD.
Company Reg. No: 05886806.
Registered in: England.

www.timeware.co.uk
support@timeware.co.uk
+44 (0) 1706 658222

4. Tenant Data Isolation

- All domain entities are tenant-scoped, enforced by EF Core query filters.
- Sharded multi-tenancy (Azure SQL Elastic Scale) partitions data by tenant ID.
- Automated build pipeline tests ensure no cross-tenant data access.

5. Audit & Retention

- Forensic audit logs capture user actions, old/new values, and affected columns.
- Hard-delete prevention; soft-deletes purged after retention periods.
- Immutable SQL-level audit logs with WORM policy.
- Configurable data retention and scheduled purging of soft-deleted data.

6. System Architecture

- Blazor WebAssembly client, monolith API, and SignalR hub for real-time communication.
- Dedicated processors for events, batch jobs (e.g., timesheets), media, and reports.
- Health-check endpoints monitor dependencies (SQL, Service Bus, Redis, Storage) for early fault detection.

7. Integrations

- Suprema biometric devices (fingerprint, face, card readers) via Suprema G-SDK.
- BioStar 2 integration for access control synchronisation.
- Sage payroll integration and developer API (REST + webhooks) for third-party systems.

8. Technology Stack:

- .NET 10 on the latest LTS framework.
- Blazor WebAssembly for the customer-facing UI, served from Azure Blob Storage.
- Entity Framework Core for data access.
- MassTransit on Azure Service Bus for messaging.
- Hangfire and Quartz.NET for background jobs.
- SignalR with Azure SignalR Service for real-time updates.
- Azure Cache for Redis for caching.
- Sentry for error tracking - data is stored in the EU (Frankfurt region). This Sentry feature is configurable per tenant - organisations can choose to enable or disable it based on their preference.

www.timeware.co.uk
support@timeware.co.uk
+44 (0) 1706 658222

9. Compliance

- Compliance with UK GDPR, ISO 27001:2022, and Cyber Essentials Plus.
- Customer data is stored and processed solely in the UK.
- Data is encrypted in transit (TLS 1.2+) and at rest (AES-256 TDE).
- Access to production data is restricted to authorised timeware UK Ltd personnel and logged.
- Configurable retention, 35-day point-in-time restore, long-term backups.
- Regular penetration testing and security assessments.

www.timeware.co.uk
support@timeware.co.uk
+44 (0) 1706 658222