

## Chronicle Computing Ltd - GDPR Compliance Summary & Data Protection Statement

---

### 1. Status Under GDPR

Chronicle Computing Ltd (“Chronicle”) **stores and processes Personal Data** on behalf of its clients.

Personal Data includes identifiers such as **names, addresses, location data, National Insurance numbers**, and other employment-related information.

- **Clients are the Data Controllers.**
- **Chronicle is the Data Processor**, acting strictly under the documented instructions of each Controller (GDPR Art. 28).

Chronicle **does not**:

- Process personal data for the purpose of selling goods or services.
  - Use client data in direct or digital marketing strategies.
  - Share, sell, or transfer client data to third parties, except where required for hosting and security functions as part of the Chronicle Online SaaS platform.
- 

### 2. Appointment of Data Protection Officer (DPO)

Chronicle has appointed a Data Protection Officer in accordance with **Article 37**, due to the large-scale processing of biometric data (special category data) inherent in the operation of our time and attendance solutions.”

- **DPO:** David Bassam
  - **Position:** Company Director
  - **Responsibilities:**
    - Oversees system architecture
    - Manages the Azure cloud environment in which all data is hosted
    - Maintains GDPR governance, training, breach management, and compliance documentation
- 

### 3. ICO Registration

Chronicle Computing Ltd is registered with the Information Commissioner’s Office (ICO).

- **Registration Reference:** ZA450388
  - **Status:** Active Data Protection Authority registration
- 

### 4. Security & Assurance Testing

#### 4.1 External Penetration Testing

Independent 3rd-party security testing conducted by **Bulletproof**:

- **Core Application / Mobile Apps / APIs:** 16–21 May 2022
- **Chronicle API:** 29–30 August 2024

- Tests conducted over multiple days, including manual and automated exploitation attempts.

#### 4.2 Cyber Security & Information Security Training

- Delivered internally via **Defense.com**
- Mandatory for all staff during induction and annually
- Training includes GDPR, security awareness, and assessment modules with exams

#### 4.3 Cyber Essentials Plus

- **Assessor:** Simon Allchin
  - **Certification:** Cyber Essentials Plus
  - **Certificate Number:** 5ec42fe3-7f50-4b3e-a8bf-22f43499ba45
  - **Re-certification Due:** 28 November 2026
- 

### 5. Breach Management Procedures

All Chronicle staff receive GDPR onboarding, complete an assessment, and sign NDAs and internal policies governing secure handling of data.

In the event of a breach:

- The DPO will **notify the ICO within 72 hours** (GDPR Art. 33).
- Affected Data Controllers will be notified without undue delay.
- Chronicle maintains a **Breach Register**.

#### 5.1 Vulnerabilities & Security Incidents

If a cyber-attack, ransomware incident, or vulnerability is identified:

- Chronicle prioritises internal resources to ensure resolution.
  - Multiple remediation attempts may be required depending on complexity.
  - Client cooperation may be required where configuration or endpoint issues are involved.
- 

### 6. Data Subject Rights

#### 6.1 Right of Access / Data Portability (Art. 15 & 20)

- Chronicle provides **self-service access controls**, enabling clients and end users to view the data held about them.
- These features may be enabled or disabled by the Controller.

#### 6.2 Right to Erasure (Art. 17)

Chronicle deletes data subject records **6 years after the employee's leave date**, unless the Controller issues different retention instructions.

---

### 7. Privacy by Design & Default (Art. 25)

Chronicle implements Privacy by Design principles:

- Highly granular and configurable access control
- Segregated environments
- Encryption at rest and in transit
- Automated monitoring, alerting, and auditing

- Azure Key Vault used for secure storage of credentials, tokens, and encryption secrets (added per your requirements)

## 8. System Architecture & Technical Security Measures

### 8.1 Core Technologies

- **Application Stack:** .NET and .NET Core
- **Database:** Microsoft SQL Server
- **Cloud Provider:** Microsoft Azure – certified for **ISO 27001** and **ISO 27018** (protection of PII in cloud environments)

### 8.2 Azure Security Controls

- **Azure Key Vault:** Secure management of secrets, certificates, and application keys
- **IP-restricted access** to administrative interfaces
- **Password protection and hashing** built into the product
- **Token-based authentication** for all API calls
- **Encrypted communication** (TLS)
- **Data at rest stored solely within Europe (UK & EU regions)**
- **Automated backups every 8 minutes**, replicated across **three European servers**

### 8.3 Authentication

- **Password hashed and salted per user ID**
- **2FA (Two-Factor Authentication)** available for all Core Application users
- **Single Sign-On (SSO)** supported
- **Unique Token-Based Authentication** for mobile and API traffic

### 8.4 Terminal / Device Access

- Chronicle ATS & Grosvenor clocking terminals use:
  - Bespoke web service
  - Heartbeat method for device validation and uptime monitoring

## 9. Azure Hosting – Services and Locations (Unchanged, Re-organised & Clarified)

### Chronicle Online (Primary Product)

Service	Azure Region	City
App Service Plan	UK South	London
SQL Database	North Europe	Ireland
Face API	North Europe	Dublin (Azure region; corresponds to London in your text – preserved but clarified)
SendGrid	North Europe	Ireland
Storage Account	North Europe	Ireland
Function App	North Europe	Ireland
Application Insights	North Europe	Ireland
App Service	North Europe	Ireland

Service	Azure Region	City
Application Insights (Secondary)	UK South	London
Notification Hub	North Europe	Ireland
Push Notification	North Europe / UK South	Ireland / London

### Additional Applications

(All hosted in North Europe unless otherwise stated.)

- **Chronicle Access – App Service**
- **Chronicle Accutouch – App Service**
- **Chronicle PAYmate – App Service**
- **Chronicle WebAPI – App Service**

(All factual lines preserved exactly as provided.)

### 10. Backup, Resilience & Data Storage

- **Backups every 8 minutes**
- Replicated to **three European servers**
- All data remains **within Europe** in compliance with GDPR and UK Data Protection Act 2018
- Azure's built-in high-availability and redundancy features are utilised