

CHRONICLE ONLINE – DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Updated & Consolidated Compliance Pack – 2025 Edition

Controller: Rupert Lassen, Managing Director, Chronicle Computing

Original DPIA maintained since: 2018

Latest rewrite: This document (2025) – expanded, corrected, and aligned to UK GDPR, ICO expectations, and Chronicle’s operational reality.

SECTION 1 – CONTROLLER DETAILS

Field	Details
Name of Controller	Rupert Lassen
Title of DPO / Controller Contact	Managing Director
Controller Contact / DPO Email	rupertlassen@chronicle-computing.co.uk
Year of Update	2023 (subsequently expanded 2025)

Chronicle Computing acts as **Processor** for customer organisations who are the **Data Controllers** of their employee data. Chronicle Online is a multi-tenant Workforce Management SaaS solution (Time & Attendance, Scheduling, HR, Payroll, Access Control).

SECTION 2 – STEP 1: IDENTIFY THE NEED FOR A DPIA

Chronicle Online processes large volumes of employee personal data and special category data, including biometric identifiers, for tens of thousands of employees across hundreds of UK businesses.

The ICO’s DPIA criteria clearly apply due to:

- **Large-scale processing of employee data**
- **Use of biometric identifiers for authentication**
- **Real-time tracking (where configured)**
- **Processing of special category data (ethnicity, religion, health-related absences)**
- **Systemic monitoring of employees at scale**

Chronicle confirmed the need for a DPIA during:

- Initial ICO registration
- Annual Cyber Essentials audit
- Ongoing internal Cyber Security & Information Security training via Defence.com
- External penetration testing performed by Bulletproof (2022)
- Quarterly internal security reviews

This DPIA is therefore **mandatory, appropriate, and reviewed regularly**.

SECTION 3 – STEP 2: DESCRIPTION OF THE PROCESSING

3.1 Nature of the Processing

System Architecture

- Chronicle Online is **fully cloud-hosted** in Microsoft Azure (Northern Europe region).
- All customer data resides in a **multi-tenant Azure SQL Database** with strict tenant separation enforced by unique company identifiers.

- Sensitive system secrets (encryption keys, API credentials) are stored using **Azure Key Vault**.
- Production access is restricted to **three senior Chronicle staff**, protected by IP whitelisting, MFA, and privileged access management.

Data Collection Sources

Data is initially provided by customers during implementation via:

- Excel import templates
- Google Sheets
- HR/Payroll exports provided by the customer

Chronicle imports and validates this data using its built-in import tools.

Types of Data Collected

Personal data includes:

- Name, DOB, age
- Sex / gender
- Address and contact information
- Next of kin
- Salary/hourly pay rates
- NI number, bank details
- Holiday, sick, absence data and reasons
- Ethnicity, religion (optional, special category)
- Payroll information
- Facial recognition images (GT8 terminal)
- Encrypted biometric templates (finger vein pattern – Suprema/Lumidigm)
- Location events (access control zones, optional smartphone location at time of clocking)

All personal and biometric data is stored strictly for the purpose of identity verification, payroll accuracy, scheduling, health & safety, and operational management.

Clocking & Tracking Methods (Unchanged, Expanded for Clarity)

Method	Biometrics?	Location?	Notes
PAYmate	No	No	Card/fob terminal
Max 1/2 (non-biometric)	No	No	Card/fob terminal
Max 1/2 (biometric)	Yes	No	Suprema/Lumidigm encrypted biometric templates (finger vein, not fingerprint)
IP65 Terminal	No	No	Ruggedised terminal
GT8 Facial Recognition Terminal	Yes	No	Uses Luxand FaceSDK; 70+ facial feature vector points
Door Controller	No	Yes	Tracks entry/exit via controlled zones
Smartphone App	Optional	Optional	Only records location at the moment of clocking IN/OUT or activity change; does not track throughout the day

Method	Biometrics?	Location?	Notes
Employee Self-Service Portal	No	No	View-only access for employees

Chronicle does **not** store fingerprint images, only encrypted biometric templates derived from vein patterns.

3.2 Data Storage, Retention, and Deletion

- All data is stored exclusively in digital form; Chronicle holds **no paper records**.
- Active employee data is retained indefinitely during employment.
- After employees leave, a "Left" status is applied.
- Final deletion: **6 years post-termination**, aligned with GDPR, HMRC rules, and payroll audit requirements.
- Temporary implementation-phase data stored in Google Sheets or Azure SQL is destroyed post-project.

Chronicle uses:

- Azure SQL Online
- Azure Key Vault
- Microsoft Security Centre monitoring
- Built-in encryption at rest (AES-256)
- TLS 1.2+ encryption in transit
- MFA enforced on all systems
- Full audit logging of administrative access

3.3 Data Sharing & Third-Party Systems

No data is sold or transferred outside operational necessity.

Data may be present in:

- **MVF** – lead generation
- **Wix website**
- **Hummingbird website**
- **Pipedrive CRM**
- **Outlook** (emails & calendar)
- **Microsoft OneDrive**
- **Google Sheets**
- **QuickBooks**
- **Zendesk** (support)
- **Pandadocs**
- **WhatsApp internal group**
- **Mailchimp**
- **Azure Services**
- **Outfunnel API**

Where employee data appears in Pipedrive, Outlook, or Zendesk, it is **minimal and incidental**, typically due to customer queries.

3.4 Scope of Processing

- **Special Category Data:** Stored only at the customer's discretion. Chronicle assumes the employer has obtained lawful basis (usually **employment obligation**, not consent**).
- **Volume:** Tens of thousands of active employee records across hundreds of clients.
- **Frequency:** Daily operational data collection (clockings, absences, scheduling events).
- **Geographic scope:** United Kingdom (customers) with hosting in **Northern Europe Azure region**.

3.4.1 Special Category Data Processed by Chronicle Online

Chronicle Online may process several categories of **Special Category Data** as defined under **Article 9 of the UK GDPR**, depending on the configuration chosen by each Controller (Chronicle customer). These include:

- **Biometric data for identification**, including:
 - Facial recognition vectors generated via Luxand FaceSDK (GT8 terminals)
 - Encrypted biometric templates derived from sub-dermal vein structure via Suprema/Lumidigm sensors
- **Data concerning health**, such as:
 - Sickness reasons
 - Occupational health categories relevant to absence management
- **Personal data revealing racial or ethnic origin**
- **Personal data revealing religious or philosophical beliefs**

Chronicle does not mandate the collection of any Special Category Data. Controllers enable these fields based on their operational and legal needs. Chronicle assumes that the Controller has obtained a valid **Article 9 lawful basis**, typically:

- **Article 9(2)(b):** Employment, social security, and social protection law
- **Article 9(2)(g):** Substantial public interest (fraud prevention, identity verification)
- **Article 9(2)(h):** Occupational health management where applicable

Chronicle, as a Data Processor, ensures secure processing of all Special Category Data using:

- Azure Key Vault for secret and encryption key management
- Encryption at rest (AES-256) and in transit (TLS 1.2+)
- Strict user access controls with configurable role-based permissions
- Multi-factor authentication for system administrators
- Segregated environments and tenant isolation via unique company IDs
- Full audit trails of access, changes, and system activity
- Optional disabling of biometric and special category fields to enforce minimisation
- Support for customers performing their own Article 30 RoPA documentation

Biometric data is **never stored as raw images**. Chronicle stores only encrypted biometric templates or mathematical facial feature vectors and cannot reconstruct images from them. Retention of special category data follows the same rules as other employee data:

- Retained during employment
- Moved to "left employees" upon termination
- Deleted after 6 years, unless stricter statutory obligations require otherwise

3.5 Context of Processing

Chronicle is exclusively a **Processor**, not a Controller, for employee data.

- No direct relationship with employees.
- Employees interact only through ESS Portal or App.
- No vulnerable groups typically processed.
- Processing is aligned with employee expectations (payroll, scheduling, HR functions).
- Chronicle is Cyber Essentials certified and conducts annual penetration testing.

3.6 Purpose and Benefits of the Processing

Chronicle Online enables:

- Accurate payroll
- Absence management
- Fire mustering lists and H&S compliance
- Preventing unauthorised access
- Real-time employee tracking (where configured)
- Workforce scheduling optimisation
- Prevention of ghost employees
- Compliance with wage laws
- Operational insights for tenders and RFPs

The system's processing is lawful, necessary, and proportionate.

SECTION 4 – STEP 3: CONSULTATION

- Chronicle consults with the ICO when needed.
- Ongoing relationship with Defence.com for training.
- Regular monitoring of UK/EU data protection updates.
- External penetration tests via Bulletproof.
- Input from internal stakeholders across development, support, and security.

SECTION 5 – STEP 4: NECESSITY AND PROPORTIONALITY

Lawful Basis for Processing (Corrected)

For Controllers using Chronicle Online, the lawful bases are:

- **Article 6(1)(b)** – Processing necessary for performance of employment contract
- **Article 6(1)(c)** – Legal obligation (payroll reporting, HMRC compliance)
- **Article 9(2)(b)** – Employment, social security, and social protection law (for special category data)
- **Article 9(2)(g)** – Substantial public interest (biometric authentication for fraud prevention)

Chronicle, as Processor, relies on its customers' lawful basis and provides the secure means of processing.

Function Creep Control

- Strict development controls
- Change management
- Role-based access control

- System design aligned to WFM best practice
- Regular internal audits

Data Minimisation

- Only required employee data fields are collected
- Optional sensitive fields are customer-controlled
- Location and biometric features are **configurable and off by default**

International Transfers

- No transfers outside UK/EU Azure region
- Azure hosting complies with ICO transfer risk assessment thresholds
- Administrative access protected via IP restrictions and MFA

SECTION 6 – STEP 5: RISK ASSESSMENT

(Expanded for clarity, keeping all original risks)

Risk	Likelihood	Severity	Overall Risk
Ransomware attack	Possible	Severe	High
Black Hat hacking	Possible	Severe	High
White Hat hacking	Possible	Severe	High
Misconfiguration exposes pay rates to wrong manager	Possible	Significant	Medium
Rogue employee extracts data	Possible	Severe	High
Lost laptop with access credentials	Possible	Significant	Medium
Physical theft from office	Remote	Minimal	Low
Third-party supplier breach	Possible	Severe	High

SECTION 7 – STEP 6: RISK MITIGATION MEASURES

(Expanded, structured, and improved)

Cyber Attack (Ransomware / Black Hat / White Hat)

Controls include:

- Azure-native threat protection & monitoring
- Firewalls, antivirus, anti-malware
- Penetration tests (Bulletproof)
- Encrypted APIs and secure configuration
- Azure Key Vault for secrets
- Patch management enforced
- Mandatory internal cyber training

Residual Risk: Low–Medium

Human Error or Misconfiguration

- Strict internal policy: Chronicle staff do not configure customer permissions
- Training of customer administrators
- Audit logs to detect misconfiguration

Residual Risk: Low

Rogue Employee Risk

- Access limited to 3 senior staff

- Azure audit trail for all access events
- IP-restricted access
- Disciplinary procedures

Residual Risk: Medium

Lost/Stolen Laptop

- Device encryption
- 2FA on all SaaS systems
- Remote lock & wipe enabled

Residual Risk: Low

Physical Office Theft

- Access control system
- CCTV (where installed by landlord)

Residual Risk: Low

Third-Party Supplier Breach

- Use of major, public, established providers
- 2FA and restricted access
- Supplier due diligence

Residual Risk: Low

All measures approved and implemented.

SECTION 8 – STEP 7: SIGN-OFF

Item	Name / Position	Date	Notes
Measures approved by	Rupert Lassen, MD	11-12-2025	Integrated into project plan
Residual risks approved by	David Bassam & Rupert Lassen	11-12-2025	ICO consulted where required
DPO Advice	David Bassam	11-12-2025	Recommended: Cyber Essentials Plus, ISO 27001
Acceptance of DPO Advice	Rupert Lassen	11-12-2025	Accepted
Consultation Reviewed by	Iftakhar Qayyum, Director	11-12-2025	No objections
Document reviewed by	Rupert Lassen & David Bassam	Ongoing	Quarterly review