

# Workwell North America Data Retention Policy

## 1. Purpose and Scope

This Data Retention Policy establishes guidelines for managing, storing, and removing data collected and processed by Eastridge Workforce Management (EWM) in its capacity as a workforce management service provider. This policy applies globally to all data operations regardless of geographic location, adhering to the most stringent requirements across international jurisdictions.

## 2. Data Classification

Eastridge Workforce Management (EWM) collects and processes the following data categories:

### 2.1 Personal Data

- Employee/contractor identifying information
- Contact information
- Professional qualifications and credentials
- Employment history and records
- Time and attendance records
- Assignment information

### 2.2 Account Data

- User credentials
- Access logs
- System usage records
- Configuration settings

### 2.3 Client Business Data

- Organizational structures
- Vendor management information
- Project and contract details
- Financial and billing information

### 2.4 System Data

- Technical logs
- Performance metrics
- Audit trails
- Error reports

## 3. Retention Periods

To ensure compliance with the most stringent global requirements, EWM adopts the following universal retention periods:

Data Type	Retention Period	Statutory Basis
Employment contracts, personnel & training records	During engagement + 7 years after termination	UK, EU GDPR, and global financial regulations

Data Type	Retention Period	Statutory Basis
Payroll, tax and wage records (including overtime, bonuses, expenses)	During engagement + 7 years after termination	Six-year requirement in UK/EU; seven years for US IRS
Current bank details	During engagement + 6 months after termination	Data minimization principle
Time and attendance records	During engagement + 7 years after termination	Tax authority requirements across jurisdictions
Work email account contents	During engagement + 6 years after termination	Legal requirements for business communications
Annual leave/vacation records	During engagement + 7 years after termination	Six years or longer where leave has been carried over
Accident, injury, or incident reports	During engagement + 4 years after termination	Three-year minimum in UK/EU; OSHA requirements in US
Working time compliance records	During engagement + 4 years after termination	Two-year requirement in EU, extended for global compliance
Immigration/work authorization checks	During engagement + 4 years after termination	Two-year minimum after employment termination
Unsuccessful job applicant data	Maximum 6 months after collection	GDPR and global privacy regulations
Background check results	During engagement (only if fact of clearance)	Data minimization principle

#### 4. Retention Justification

These retention periods are established based on:

- Employment and labor law requirements across all jurisdictions including UK, EU, US, Canada, and Asia-Pacific
- Tax and financial record-keeping obligations (up to 7 years for IRS and other tax authorities)
- Contractual requirements and commercial necessity
- Limitation periods for potential claims (typically 6-7 years in most jurisdictions)
- Data minimization principles under GDPR, CCPA/CPRA, and global privacy regulations

#### 5. Data Storage and Security

##### 5.1 All retained data shall be stored with appropriate security measures including:

- Encryption at rest and in transit using industry-standard protocols
- Access controls based on least privilege principle
- Regular security assessments and monitoring
- Segregation of data categories
- Geographic data residency considerations where legally required

##### 5.2 Archival data shall be:

- Stored in separate, secure, and tamper-evident systems
- Accessible only to authorized personnel via documented procedures
- Subject to periodic integrity verification
- Protected by additional safeguards for cross-border transfers where applicable

## **6. Data Deletion**

### **6.1 Automatic Deletion**

- At the conclusion of the applicable retention period, data shall be automatically flagged for deletion
- Deletion shall be irreversible and complete, including from backup systems
- Technical logs shall document all deletion activities

### **6.2 Early Deletion Requests**

- Data subjects may request earlier deletion under applicable privacy laws (GDPR, CCPA/CPRA, etc.)
- Active clients requesting deletion will have non-essential data deleted while service-critical data will be minimized
- Requests will be evaluated against legal hold obligations and regulatory requirements
- Approved requests will be executed within 30 days (or within 45 days for CCPA/CPRA compliance)
- Clear documentation will be provided regarding what was deleted and what was retained (with justification)

### **6.3 Legal Holds**

- Data subject to legal proceedings, investigations, or regulatory requirements will be exempt from standard deletion
- Legal holds must be documented, reviewed quarterly, and removed promptly when no longer applicable
- Legal holds take precedence over deletion requests but must be justified and minimized

## **7. Data Minimization and Processing Limitations**

**7.1** EWM will collect and retain only data necessary for legitimate business purposes in alignment with global data protection laws.

**7.2** Personal data will be de-identified or pseudonymized where feasible for analytical purposes, though this does not substitute for deletion when requested.

**7.3** Access to retained data will be restricted to personnel with legitimate business needs through role-based access controls.

**7.4** Special categories of personal data (sensitive data) will receive enhanced protection and minimization.

## **8. Compliance and Documentation**

**8.1** EWM will maintain records of:

- Data processing activities
- Data deletion activities
- Legal hold implementation and removal
- Access to archived data
- Data subject requests and resolutions
- Data protection impact assessments where applicable

**8.2** This policy shall be reviewed annually and updated as needed to reflect changes in:

- Legal requirements across all jurisdictions
- Business operations
- Technology capabilities
- Best practices for data protection
- Emerging privacy standards

## **9. Client Data Return**

**9.1** Upon contract termination, clients may request:

- Return of all client data in standard, machine-readable format
- Certificate of deletion following data return
- Immediate deletion of non-essential data upon request, even during active service

**9.2** Client data return requests must be submitted within 30 days of contract termination.

**9.3** For clients in jurisdictions with specific data sovereignty requirements, data return will comply with local regulations.

## **10. Exceptions and Special Considerations**

**10.1** Any exceptions to this policy must be:

- Approved by the Chief Operating Officer
- Documented with written justification
- Reviewed quarterly
- Limited to the minimum necessary deviation

**10.2** Additional considerations for specific jurisdictions:

- EU/UK: Enhanced GDPR rights implementation
- California: CCPA/CPRA compliance for deletion requests
- Canada: PIPEDA requirements for consent and retention
- International transfers: Appropriate safeguards for cross-border data flows

## **11. Policy Enforcement**

**11.1** All EWM employees and contractors must comply with this policy.

**11.2** Violations may result in disciplinary action up to and including termination.

**11.3** Regular audits will verify compliance with this policy across all operations globally.

**11.4** Annual training on data protection requirements will be provided to all staff.

## **12. Contact Information**

For questions or concerns regarding this policy, contact:

Global Data Protection  
Eastridge Workforce Management  
privacy@eastridgewm.com

---

**Last Updated:** April 18, 2025  
**Version:** 3.0