Privacy Policy

Effective Date: 1st April 2025

1. Introduction

MintHRM is a Human Resources SaaS platform committed to protecting the privacy and security of personal data processed through our systems. This policy outlines how we collect, use, disclose, store, and protect personal information in accordance with ISO/IEC 27001, HIPAA, and relevant data protection laws.

2. Objective

The objective of this policy is to ensure that personal data processed through MintHRM is protected in accordance with the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). This policy outlines how MintHRM collects, processes, stores, shares, and protects personal and sensitive data.

3. Scope

This policy applies to all employees, contractors, clients, vendors, and third-party partners who access or process personal data through MintHRM systems, including web and mobile platforms. It covers:

- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Employment and HR-related data

This policy also applies to:

- Web application
- Mobile applications
- Open API integrations
- Backend systems
- Data warehouse and reporting tools

And the following user roles:

- End users (employees)
- HR administrators
- System integrators
- API clients (e.g., payroll systems, biometric attendance devices)

4. Policy Statement

MintHRM is committed to safeguarding the privacy and rights of data subjects. We collect and process personal data lawfully, fairly, and transparently. All data is used strictly for the purposes communicated to the data subjects and in line with applicable legal requirements.

5. Data Collection and Usage

- Personal data is collected only for legitimate, specific, and clearly defined purposes.
- Data includes identifiers such as names, contact details, employment data, and where applicable, health-related information under HIPAA.
- Legal bases for processing include user consent, contractual necessity, legal obligations, and legitimate interests.
- Data is not used for unrelated purposes without further consent.
- Sensitive data, especially health information, is handled under strict compliance with HIPAA guidelines.

Data Category	Example Data Types	Purpose of Collection	Legal Basis
Identifiers (PII)	Name, NIC/Passport number, Employee ID, Date of Birth	User identification, employee profile management	Contractual necessity, Legitimate interest
Contact Information	Email, Phone number, Home address	Communication, payroll processing, emergency contact	Contractual necessity, Consent
Employment Data	Job title, Department, Work location, Joining date	HR management, organizational hierarchy	Contractual necessity, Legitimate interest
Attendance & Time Data	Clock-in/out times, GPS location, Shift schedules	Time tracking, attendance management, compliance	Legitimate interest, Legal obligation
Leave & Absence Data	Leave types, Leave dates, Approval status, Medical certificates	Leave management, workforce planning, compliance	Consent, Legal obligation (labor law)
Payroll & Benefits Data	Salary, Allowances, Deductions, Bank account number	Salary disbursement, tax compliance	Contractual necessity, Legal obligation
System Usage Data	Login times, IP address, API logs, Device type	Security, audit trails, service improvements	Legitimate interest, Legal obligation

Sensitive Health Data (PHI)	Doctor's notes, Diagnosis, Medical leave reason, Vaccination status	Medical leave validation, workplace health compliance (if applicable)	Consent, Legal obligation (HIPAA)

6. Document Security Classification

MintHRM classifies information based on sensitivity and access level:

Classification	Description	Examples
Public	No restrictions on access or sharing.	Public API docs, website content
Internal Use Only	Only accessible by MintHRM employees and contractors.	Internal training material, dev docs
Confidential	Limited to specific roles; requires approval for sharing.	HR policies, client setup details
Restricted / Highly Confidential	Strictly controlled; includes PII and PHI.	Employee payroll, medical data, access logs

Security Controls by Classification:

- RBAC enforcement
- Encryption standards
- Audit logging
- Data retention & disposal procedures

7. Non-Compliance

Non-compliance with this policy, whether intentional or accidental, may lead to disciplinary action, legal consequences, and/or termination of employment or contract. Data breaches are reported according to GDPR/HIPAA timelines and protocols.

8. Roles and Responsibilities

To maintain effective data privacy and security, the following roles are defined:

Employees:

- Must follow internal data privacy policies.
- Are responsible for safeguarding their credentials.
- Should report any suspected data breach or suspicious system activity immediately.

Managers:

- Ensure that their teams are trained on data privacy policies.
- Validate that employees are granted appropriate system access aligned with their roles.
- Escalate potential privacy risks to the DPO or IT teams.

Data Protection Officer (DPO):

- Oversees data protection strategy and implementation.
- Reviews and updates the privacy policy in line with legal and regulatory changes.
- Acts as the liaison with data protection authorities and manages subject access requests (SARs).
- Coordinates periodic privacy impact assessments (PIAs) for new or updated features.

IT and Security Teams:

- Implement and maintain technical safeguards, including encryption, firewalls, and monitoring systems.
- Regularly review access logs, suspicious activity, and intrusion alerts.
- Ensure that infrastructure and software are patched and up-to-date.
- Conduct internal audits and coordinate third-party penetration testing.

9. Client Responsibilities

- Determining the lawful basis for processing personal data under applicable legal frameworks (e.g., consent, contract, legal obligation, legitimate interest).
- Providing transparency notices to employees and ensuring they are informed of how their data will be used.
- Obtaining necessary consents from data subjects, particularly for sensitive data (e.g., health information under HIPAA or biometric data).
- Responding to data subject rights requests (access, rectification, deletion, objection, portability).
- Defining and configuring appropriate Role-Based Access Control (RBAC) settings and user permissions within the MintHRM system.
- Maintaining records of processing activities where required by data protection laws.

MintHRM, as a data processor, provides system features to support clients' compliance efforts, including audit logs, user access controls, and secure APIs.

10. Data Retention

We retain personal data only for the duration necessary to fulfill the purposes above, subject to:

- Data Type
- Retention Period
- Attendance & Leave
- 7 years (audit/compliance)
- Payroll
- 7 years (financial compliance)
- Employee Profile
- Until employment ends + 3 years
- Activity Logs
- 1 year (security monitoring)

11. Breach Notification

In the event of a data breach affecting personal data, MintHRM will notify affected clients within 72 hours of becoming aware of the incident. The notification will include:

- Nature and scope of the breach.
- Types of data affected.
- Likely consequences for individuals and clients.
- Measures taken or proposed to address the breach and mitigate its effects.
- MintHRM will provide support to clients in notifying relevant authorities (e.g., Data Protection Authorities) and impacted individuals, as required.
- A full post-incident report will be shared with clients, and necessary corrective actions will be tracked and implemented.

12. Schedule

- Policy Review: Annually, or in response to legal or operational changes.
- Training: Conducted for all staff during onboarding and refreshed annually.
- Audits: Bi-annual privacy audits to ensure ongoing compliance with GDPR and HIPAA.

End of Access Control Policy. For version history, please see the next page.

Version history

Version	Log	Date
	No version history available	