PAYROLLPRO DATA PROTECTION POLICY

Effective Date: October 01, 2020
Last Updated: July 01, 2026
Document Owner: Data Protection Officer / Privacy Office
Company: Analytics and Data Integrity, Inc., doing business as PayrollPRO / PayrollPRO.PH / ADIConsulting

1. Policy Statement

Analytics and Data Integrity, Inc., doing business as PayrollPRO, PayrollPRO.PH, and ADIConsulting ("PayrollPRO," "ADI," "Company," "we," "us," or "our"), is committed to protecting the confidentiality, integrity, availability, and lawful use of personal data entrusted to us.

PayrollPRO provides HRIS, employee records, timekeeping, attendance, payroll, government reporting, employee servicing, onboarding, offboarding, final pay, managed payroll, deployment, support, and related technology services. These services may involve the processing of personal information, sensitive personal information, privileged information, payroll records, attendance data, government identifiers, statutory contribution data, employment records, and other confidential business information.

This Data Protection Policy sets out the principles, controls, responsibilities, and procedures that PayrollPRO follows to protect personal data in accordance with the **Data Privacy Act of 2012**, its Implementing Rules and Regulations, and relevant issuances of the National Privacy Commission. The Data Privacy Act protects individual personal information in information and communications systems in both government and private sectors. (Lawphil)

---

2. Purpose of this Policy

This Policy is intended to:

a. establish PayrollPRO's data protection standards;
b. define how personal data is collected, used, stored, shared, retained, secured, and disposed of;
c. clarify PayrollPRO's responsibilities as a Personal Information Controller and/or Personal Information Processor;
d. guide employees, officers, contractors, support staff, developers, administrators, and authorized representatives in handling personal data;
e. protect Client data, employee data, payroll data, HR records, attendance records, and system data;
f. support compliance with the Data Privacy Act, contractual obligations, and professional standards; and

g. provide a framework for responding to data subject requests, data incidents, security incidents, and personal data breaches.

---

3. Scope

This Policy applies to all personal data processed by PayrollPRO, whether collected, stored, accessed, hosted, transmitted, generated, modified, archived, deleted, or otherwise processed through:

a. PayrollPRO websites, landing pages, demo forms, inquiry forms, and marketing channels;
b. PayrollPRO HRIS, employee records, 201 files, document management, policies, announcements, employee servicing, onboarding, offboarding, and performance modules;
c. PayrollPRO timekeeping, attendance, leave, overtime, schedule, holiday, night differential, rest day, web tracker, mobile attendance, biometric integration, DeviceHub, and attendance dispute functions;
d. PayrollPRO payroll, payroll register, payslips, deductions, allowances, benefits, loans, final pay, government report generators, statutory contribution reports, bank files, and payroll analytics;
e. support, deployment, implementation, migration, parallel testing, training, account management, technical consultation, and troubleshooting activities;
f. outsourced payroll, managed payroll, lodgment support, employer-of-record support, and related services where separately agreed;
g. PayrollPRO internal operations, personnel records, contractor records, vendor records, and business records; and
h. connected systems, APIs, hosting providers, support tools, communication tools, and third-party services used to deliver PayrollPRO services.

This Policy applies to all PayrollPRO directors, officers, employees, contractors, consultants, developers, support personnel, agents, partners, subprocessors, vendors, and authorized representatives who process or access personal data on behalf of PayrollPRO.

---

4. Data Protection Roles

PayrollPRO may act in different roles depending on the processing activity.

4.1 PayrollPRO as Personal Information Controller

PayrollPRO acts as a Personal Information Controller when it determines the purpose and means of processing personal data, including for:

a. website inquiries and demo requests;
b. client contact persons and account management;
c. marketing, newsletters, business development, and partnership communications;
d. billing, invoices, contracts, statements of work, and payment records;
e. PayrollPRO user account administration;
f. support tickets and service communications;
g. internal employment, contractor, vendor, and administrative records;
h. legal, accounting, tax, audit, compliance, and business records; and
i. security monitoring, fraud prevention, and system protection.

4.2 PayrollPRO as Personal Information Processor

PayrollPRO generally acts as a Personal Information Processor when it processes employee, HR, payroll, attendance, timekeeping, biometric/device, government-reporting, and Client-controlled operational data on behalf of a Client.

In this role, PayrollPRO processes data based on the Client's instructions, subscribed package, system configuration, service agreement, order form, statement of work, support request, or Data Processing Agreement.

The Client remains responsible for the lawful collection, accuracy, notices, consents, employment basis, company policies, payroll rules, government reporting decisions, and data subject communications relating to Client-controlled employee and payroll data.

---

5. Data Protection Principles

PayrollPRO follows the following data protection principles:

5.1 Transparency

Data subjects should be informed about the collection, use, sharing, retention, and protection of their personal data through privacy notices, policies, contracts, and appropriate communications.

5.2 Legitimate Purpose

Personal data shall be processed only for legitimate, declared, and specific purposes, including HRIS, timekeeping, payroll, government reporting, support, account management, legal compliance, and service delivery.

5.3 Proportionality

PayrollPRO shall process only the data necessary, relevant, and adequate for the declared purpose.

5.4 Accuracy

PayrollPRO shall take reasonable steps to maintain accurate system processing. However, Clients are responsible for ensuring that employee, payroll, attendance, and HR data submitted to PayrollPRO is complete, updated, and accurate.

5.5 Security

PayrollPRO shall implement reasonable and appropriate technical, organizational, and physical safeguards to protect personal data against unauthorized access, loss, misuse, alteration, disclosure, or destruction.

5.6 Accountability

PayrollPRO shall maintain governance, policies, contracts, logs, controls, training, and documentation to demonstrate responsible data protection practices.

5.7 Retention Limitation

Personal data shall be retained only for as long as necessary for the declared purpose, contract, legal requirement, audit, accounting, tax, employment, payroll, security, or dispute-resolution need.

---

6. Categories of Personal Data Processed

PayrollPRO may collect and process the following categories of data, depending on the subscribed services and the role of the data subject.

6.1 Client Contact and Business Data

a. name;
b. company name;
c. job title or role;
d. email address;
e. mobile number or telephone number;
f. office address;
g. billing details;
h. contract and account details;
i. communication history; and
j. support, implementation, and service records.

6.2 Employee and HRIS Data

a. employee number;
b. name;
c. address and contact information;
d. date of birth, civil status, gender, nationality, dependents, and family details where required by the Client;
e. employment status, position, department, branch, team, supervisor, cost center, project, and reporting line;
f. employment start date, regularization date, separation date, contract type, and employment records;
g. 201 files, contracts, IDs, certificates, memos, forms, attachments, and documents uploaded by the Client or User;
h. benefits, compensation package, leave credits, work schedule, and HR profile;
i. employee tickets, requests, approvals, disputes, acknowledgements, and system activity; and
j. other employee-related information required by the Client.

6.3 Payroll and Statutory Data

a. salary, wage, rate, allowance, bonus, commission, incentive, overtime, night differential, holiday pay, rest day pay, premium pay, deductions, reimbursements, loans, and adjustments;
b. payroll period, pay codes, payroll register, payslip, YTD details, payroll summary, and journal entry data;
c. bank account or disbursement information, where required for payroll processing;
d. TIN, SSS, PhilHealth, Pag-IBIG, and other government or statutory identifiers;
e. withholding tax information, statutory contribution records, loans, remittance references, government reports, and BIR Form 2316-related information;
f. final pay, separation pay, quitclaim-related references, offboarding payroll data, and clearance-related references; and
g. payroll-related tickets, authority to deduct, benefit requests, and adjustment records.

6.4 Timekeeping, Attendance, and Device Data

a. time-in and time-out records;
b. web tracker logs;
c. mobile attendance records;
d. geo-location or geo-verification data if enabled by the Client;
e. biometric device logs or device-generated identifiers if integrated;
f. RFID, fingerprint, facial/photo logs, card reader logs, and similar device-generated attendance data, depending on the device used and Client configuration;
g. schedule, shift, rest day, holiday, overtime, night differential, leave, tardiness, undertime, attendance summary, and exception records;
h. approval logs, dispute records, corrections, adjustments, and audit trails; and
i. device connection logs, technical metadata, and integration records.

6.5 Recruitment, Onboarding, Offboarding, Performance, and HR Servicing Data

Where the relevant modules are subscribed or enabled, PayrollPRO may process applicant records, onboarding requirements, offboarding documents, clearances, exit interview references, policy acknowledgements, performance evaluation records, KPI records, surveys, feedback, ticketing records, training records, career development data, and related HR documents.

6.6 System, Security, and Technical Data

a. usernames and user IDs;
b. hashed or encrypted credentials where applicable;
c. access rights, roles, permissions, and user status;
d. login history, IP address, browser type, device type, and operating system;
e. activity logs, audit logs, error logs, and security logs;
f. session information, cookies, and analytics data;
g. support logs and troubleshooting records;
h. backup records and archival logs; and
i. other technical data necessary for security, support, monitoring, and platform improvement.

---

7. Purposes of Processing

PayrollPRO processes personal data for the following purposes:

a. creating, administering, and securing PayrollPRO accounts;
b. providing HRIS, employee records, 201 file, document management, employee self-service, and HR servicing functions;
c. processing timekeeping, attendance, schedule, leave, overtime, holiday, rest day, night differential, tardiness, undertime, and dispute records;
d. supporting biometric device, web tracker, mobile attendance, DeviceHub, API, and system integrations where applicable;
e. processing payroll, payslips, payroll register, deductions, allowances, benefits, loans, final pay, and payroll reports;
f. generating payroll-related government reports and statutory contribution reports;
g. supporting onboarding, offboarding, policies, announcements, performance, ticketing, surveys, and other subscribed HR modules;
h. supporting deployment, data migration, process mapping, system calibration, testing, go-live, training, troubleshooting, and account management;
i. providing managed payroll, outsourced payroll, government lodgment support, or related services where separately agreed;
j. complying with legal, tax, accounting, audit, regulatory, contractual, and professional obligations;
k. maintaining security, access control, fraud prevention, audit logs, backups, and disaster recovery;
l. responding to Client requests, user requests, data subject requests, and support concerns;

m. improving PayrollPRO functionality, documentation, user experience, security, and system performance;
n. sending administrative, service, billing, support, and security communications; and
o. sending marketing or product communications where allowed by law and subject to opt-out rights.

---

8. Legal Bases for Processing

PayrollPRO processes personal data based on one or more lawful grounds, including:

a. consent of the data subject, where required;
b. contract between PayrollPRO and the Client, User, employee, vendor, or partner;
c. compliance with legal obligations under applicable Philippine laws and regulations;
d. legitimate business interests in operating, securing, improving, and supporting PayrollPRO services;
e. fulfillment of employment, payroll, HR, accounting, tax, statutory, or government reporting requirements, as instructed by the Client;
f. protection of lawful rights and interests in legal claims, audits, investigations, incident response, or dispute resolution; and
g. other lawful bases recognized under applicable data protection laws.

For Client-controlled employee, HR, payroll, and attendance data, the Client is primarily responsible for determining, documenting, and communicating the applicable lawful basis to the data subject.

---

9. Data Sharing and Disclosure

PayrollPRO does not sell, rent, or trade personal data.

PayrollPRO may share or disclose personal data only when necessary, lawful, and appropriate, including:

9.1 Authorized Client Representatives

PayrollPRO may make data available to Company Admins, HR users, payroll users, managers, approvers, employees, auditors, accountants, and other authorized representatives designated by the Client.

9.2 Government Agencies and Legal Requirements

PayrollPRO may process, generate, or disclose data to government agencies or portals, such as BIR, SSS, PhilHealth, Pag-IBIG, DOLE, or other authorities, where required by law, contract, Client instruction, or subscribed service.

9.3 Service Providers and Subprocessors

PayrollPRO may engage reputable service providers and subprocessors, such as hosting providers, cloud infrastructure providers, communication tools, analytics tools, support tools, security tools, payment processors, backup providers, system monitoring tools, and professional advisers.

Such service providers shall be required, where applicable, to process data only for authorized purposes and to observe contractual, confidentiality, security, and data protection obligations.

9.4 Professional Advisers

PayrollPRO may disclose limited information to lawyers, accountants, auditors, consultants, tax advisers, insurers, and other professional advisers when necessary for legal, audit, accounting, tax, claims, or compliance purposes.

9.5 Business Transfers

Personal data may be disclosed or transferred in connection with a merger, acquisition, restructuring, financing, sale of assets, or similar business transaction, subject to confidentiality and data protection safeguards.

9.6 Emergency, Security, and Legal Protection

PayrollPRO may disclose information where necessary to protect rights, safety, property, systems, users, Clients, Employees, or the public, or to investigate suspected fraud, unauthorized access, illegal activity, cybercrime, or misuse.

---

10. Subprocessor and Vendor Management

PayrollPRO shall take reasonable steps to ensure that service providers and subprocessors handling personal data are selected, assessed, and managed properly.

PayrollPRO’s vendor management controls may include:

a. due diligence on security, privacy, and reliability;
b. data processing, confidentiality, or service agreements where applicable;

c. limitation of processing to approved purposes;
d. access restrictions and least-privilege controls;
e. security requirements appropriate to the risk and nature of data;
f. breach notification obligations;
g. retention and deletion requirements where applicable; and
h. periodic review of vendor performance or continued suitability.

PayrollPRO may maintain a Subprocessor List for Clients who require visibility over major service providers used in delivering PayrollPRO services.

---

11. Data Storage, Hosting, and International Transfers

Personal data may be stored in secure servers, databases, backups, cloud platforms, and authorized systems used by PayrollPRO.

Depending on the Client's service setup, personal data may be hosted in the Philippines or in other jurisdictions where PayrollPRO, its hosting providers, cloud providers, or service providers operate.

Where personal data is transferred outside the Philippines, PayrollPRO shall take reasonable steps to ensure appropriate safeguards, which may include contractual obligations, security controls, access restrictions, encryption, and vendor due diligence.

Clients requiring specific data residency, hosting location, or cross-border transfer terms should raise these requirements before subscription, implementation, or renewal so they can be addressed in the applicable agreement or Data Processing Agreement.

---

12. Data Retention

PayrollPRO retains personal data only for as long as necessary for the purpose for which it was collected or processed, or as required by contract, law, accounting, tax, employment, audit, security, dispute-resolution, or legitimate business requirements.

Retention periods may depend on:

a. active subscription period;
b. Client instructions;
c. employment and payroll record requirements;
d. tax and accounting requirements;
e. statutory contribution and government reporting requirements;
f. audit, investigation, litigation, or dispute requirements;

g. backup and disaster recovery cycles;
h. support and security log retention periods; and
i. signed service agreement, Data Processing Agreement, order form, or statement of work.

Upon termination of services, PayrollPRO may, subject to the applicable agreement and legal obligations:

a. allow the Client to export or download available data;
b. return data in a reasonable format;
c. delete, anonymize, archive, or restrict data after the applicable retention period;
d. retain limited copies for legal, tax, accounting, audit, security, backup, and dispute-resolution purposes; and
e. remove access after termination, expiration, or non-payment.

Payroll, accounting, tax, government, audit, security, and legal records may be retained longer where required or permitted by law.

---

13. Security Measures

PayrollPRO implements reasonable and appropriate organizational, technical, and physical measures to protect personal data.

These may include:

a. role-based access control;
b. least-privilege access;
c. user authentication and password controls;
d. administrative access restrictions;
e. encryption in transit and at rest where appropriate;
f. secure hosting and server controls;
g. database access controls;
h. audit logs and activity monitoring;
i. backup and disaster recovery procedures;
j. vulnerability assessment and remediation;
k. system patching and maintenance;
l. malware and threat protection where applicable;
m. secure development and change management practices;
n. confidentiality agreements for employees, contractors, and vendors;
o. privacy and security awareness training;
p. access review and account deactivation procedures;
q. incident response and breach management procedures; and
r. physical and administrative controls for office, device, and document security.

No system, internet transmission, email, device, cloud service, or integration can be guaranteed to be completely secure. Clients and Users must also maintain proper security practices, including protecting credentials, limiting access, validating user permissions, and promptly reporting suspected incidents.

---

14. Access Control and User Management

PayrollPRO follows access control principles designed to limit data access to authorized users only.

Controls may include:

a. unique user accounts;
b. role-based permissions;
c. company-level or tenant-level data separation;
d. access logs and audit trails;
e. administrative access restrictions;
f. user activation, deactivation, and role change procedures;
g. password and authentication requirements;
h. review of privileged accounts; and
i. immediate access revocation for separated personnel or unauthorized users.

Clients are responsible for managing their own Company Admins, approvers, HR users, payroll users, managers, employees, and other authorized users within their PayrollPRO account.

Clients must promptly remove or update access when a user resigns, changes role, changes department, or no longer requires access.

---

15. Biometric, DeviceHub, and Attendance Device Protection

Where a Client uses biometric devices, RFID devices, facial/photo logs, fingerprint logs, time clocks, mobile attendance, geo-verification, DeviceHub, or similar attendance integrations, PayrollPRO shall process device and attendance data only within the subscribed service and Client-approved configuration.

Clients using biometric or attendance devices are responsible for:

a. informing employees about the device or attendance technology used;
b. securing necessary consent or lawful basis where required;
c. issuing internal policies on attendance recording and device use;
d. ensuring devices are physically secured;

e. controlling enrollment, removal, and access to device records;
f. validating device logs, missed logs, duplicate logs, and attendance disputes;
g. reporting lost, compromised, defective, or unauthorized devices; and
h. ensuring that device use complies with employment, privacy, security, and workplace policies.

PayrollPRO shall apply reasonable technical and organizational safeguards to device-related data processed through PayrollPRO, but PayrollPRO is not responsible for third-party device defects, power interruptions, unsupported devices, local network failures, or Client-side misuse unless expressly agreed in writing.

---

16. Data Subject Rights

Data subjects have rights under the Data Privacy Act. The National Privacy Commission states that data subjects have the right to reasonable control over the flow of their personal data and identifies rights such as access, correction, objection, erasure or blocking, portability, damages, and complaint. (National Privacy Commission)

Subject to applicable law, verification, and lawful limitations, data subjects may exercise the following rights:

a. right to be informed;
b. right to object;
c. right to access;
d. right to rectification or correction;
e. right to erasure or blocking;
f. right to data portability, where applicable;
g. right to damages where legally available;
h. right to file a complaint with the National Privacy Commission; and
i. right to be informed of material updates to relevant privacy notices and data protection policies.

For employee, attendance, HR, payroll, benefits, statutory, 201 file, or employment-related data controlled by a Client, Employees and other data subjects should first contact their employer or the Client's authorized HR, Payroll, or Company Admin team.

PayrollPRO may coordinate with the Client to respond to data subject requests where PayrollPRO acts as a Personal Information Processor.

Where PayrollPRO acts as Personal Information Controller, requests may be sent directly to the PayrollPRO Data Protection Officer.

---

17. Procedure for Data Subject Requests

PayrollPRO shall handle data subject requests in a reasonable, secure, and documented manner.

The request procedure may include:

a. receiving the request through the Data Protection Officer or authorized channel;
b. verifying the identity and authority of the requester;
c. determining whether PayrollPRO is acting as Controller or Processor;
d. forwarding Client-controlled requests to the appropriate Client representative where necessary;
e. reviewing applicable legal, contractual, security, confidentiality, employment, and retention limitations;
f. providing access, correction, deletion, blocking, portability, or appropriate response where legally required;
g. documenting the request, action taken, and response; and
h. escalating complex, disputed, or high-risk requests to the Data Protection Officer, management, or legal counsel.

PayrollPRO may deny, defer, or limit a request where allowed by law, such as when the request is unauthorized, excessive, legally restricted, affects another person's rights, compromises security, conflicts with legal retention obligations, or relates to Client-controlled data requiring Client instruction.

---

18. Data Breach and Security Incident Management

PayrollPRO shall maintain a process for identifying, reporting, assessing, containing, investigating, documenting, and resolving security incidents and personal data breaches.

In the event of a suspected or confirmed personal data breach, PayrollPRO shall:

a. activate containment and recovery measures;
b. assess the nature, scope, affected data, affected systems, and potential harm;
c. preserve relevant evidence, logs, and records;
d. notify affected Clients where their data is involved;
e. coordinate with Clients regarding employee or data subject notification where PayrollPRO acts as Processor;
f. notify the National Privacy Commission and affected data subjects where required by law;
g. take corrective and preventive measures; and
h. document the incident, response, findings, and remediation.

PayrollPRO personnel, contractors, vendors, and authorized users must report suspected data incidents, unauthorized access, lost devices, accidental disclosures, misdirected emails,

compromised credentials, malware, system abuse, or unusual activity immediately to the Data Protection Officer or designated security contact.

---

19. Internal Responsibilities

19.1 Management

PayrollPRO management is responsible for supporting data protection governance, approving policies, allocating resources, enforcing compliance, and ensuring that privacy and security are incorporated into operations and service delivery.

19.2 Data Protection Officer

The Data Protection Officer is responsible for:

a. overseeing data protection compliance;
b. advising management and personnel on privacy obligations;
c. handling data subject requests and privacy concerns;
d. coordinating incident and breach response;
e. maintaining privacy documentation;
f. supporting privacy training and awareness;
g. coordinating with Clients, vendors, and authorities where necessary; and
h. monitoring policy updates and compliance activities.

19.3 System Administrators and Technical Team

System administrators and technical personnel are responsible for implementing access controls, security configurations, backups, monitoring, incident response, patching, troubleshooting, and technical safeguards.

19.4 Support, Payroll, HR, and Operations Personnel

Personnel handling Client data must process data only for authorized purposes, follow Client instructions, observe confidentiality, avoid unnecessary access, and report suspected incidents immediately.

19.5 Clients and Company Admins

Clients and Company Admins are responsible for lawful data collection, internal notices, employee consent or lawful basis, user access management, accurate records, payroll validation, employee communications, and compliance with their own employment, payroll, tax, statutory, and privacy obligations.

20. Privacy by Design and Default

PayrollPRO shall aim to integrate privacy and security into system design, development, deployment, configuration, and support.

This may include:

a. collecting only necessary data;
b. applying role-based access;
c. limiting default access rights;
d. segregating Client data;
e. using audit logs;
f. applying secure configuration;
g. reviewing new features for privacy impact;
h. assessing high-risk processing activities;
i. protecting sensitive payroll, government, biometric, and employee data; and
j. documenting material changes that affect personal data processing.

---

21. Training and Awareness

PayrollPRO shall provide appropriate data protection and security awareness to personnel who process personal data.

Training may include:

a. Data Privacy Act basics;
b. confidentiality obligations;
c. secure handling of payroll and employee records;
d. password and access security;
e. phishing and social engineering awareness;
f. incident reporting;
g. handling data subject requests;
h. secure file sharing; and
i. Client confidentiality and support boundaries.

---

22. Records, Documentation, and Audit

PayrollPRO shall maintain reasonable records and documentation to support compliance, including:

a. privacy policies and notices;
b. Data Processing Agreements;
c. service agreements and Client instructions;
d. data inventory or processing records where appropriate;
e. subprocessor or vendor records;
f. access logs and audit logs;
g. data subject request records;
h. incident and breach records;
i. training records;
j. risk assessments or privacy impact assessments where required; and
k. retention and deletion records where practical.

PayrollPRO may conduct internal reviews, access reviews, technical reviews, or compliance assessments to monitor adherence to this Policy.

---

23. Data Disposal and Deletion

PayrollPRO shall dispose of, delete, anonymize, archive, or restrict access to personal data when it is no longer necessary, subject to legal, contractual, audit, backup, accounting, tax, security, and dispute-resolution requirements.

Secure disposal methods may include:

a. deletion from active systems;
b. restriction of access;
c. anonymization or aggregation;
d. secure destruction of physical documents;
e. deletion from backups after backup retention cycles; and
f. documented data return or export upon Client request, where applicable.

---

24. Policy Violations

Any violation of this Policy may result in disciplinary action, access restriction, termination of access, contract remedies, legal action, or reporting to authorities, depending on the nature and severity of the violation.

Violations may include:

a. unauthorized access;
b. unauthorized disclosure;
c. credential sharing;

d. misuse of Client or employee data;
e. failure to report a data incident;
f. intentional deletion or alteration of records;
g. unlawful processing;
h. bypassing security controls;
i. use of data for unauthorized purposes; and
j. violation of confidentiality obligations.

---

25. Contact Information

For privacy concerns, data subject requests, security incidents, or questions about this Policy, please contact:

Data Protection Officer / Privacy Officer
PayrollPRO.PH by Analytics and Data Integrity, Inc.
Email: james.garcia@payrollpro.ph
Alternative Email: support@payrollpro.ph / support@adiconsulting.ph
Phone: +63 917 881 6255
Office Address: Unit 323, Vinia Building, 929 Epifanio de los Santos Ave., Philam, Quezon City, Metro Manila, Philippines
Website: https://payrollpro.ph

For employee-specific concerns involving HR records, payroll, attendance, benefits, government information, or employment data, Employees should first contact their employer's HR, Payroll, or Company Admin team.

---

26. Policy Review and Updates

This Policy shall be reviewed periodically or when there are material changes in law, PayrollPRO services, security controls, processing activities, systems, vendors, or business operations.

Updates may be communicated through the PayrollPRO website, platform notice, email, contract update, Client advisory, or other reasonable means.

The updated Policy shall take effect on the date indicated in the revised document.
