PAYROLLPRO PRIVACY POLICY

Effective Date: October 01, 2021
Last Updated: July 01, 2026

This Privacy Policy explains how **Analytics and Data Integrity, Inc.**, doing business as **PayrollPRO**, **PayrollPRO.PH**, and **ADIConsulting** ("PayrollPRO," "ADI," "we," "us," or "our"), collects, uses, stores, shares, protects, and retains personal information in connection with our websites, applications, platforms, subscription services, managed payroll services, HRIS, timekeeping, attendance, payroll, government reporting, employee self-service, support, and related products and services.

PayrollPRO is designed for businesses, employers, HR teams, payroll teams, administrators, employees, consultants, contractors, and authorized users who use PayrollPRO as a payroll, HR, timekeeping, attendance, employee record, employee servicing, and workforce management solution.

By accessing our website, registering for an account, using PayrollPRO, submitting information through the platform, or entering into a subscription, service, partnership, deployment, or support arrangement with us, you acknowledge that you have read and understood this Privacy Policy.

This Privacy Policy should be read together with our Terms of Use, Subscription Agreement, Service Agreement, Data Processing Agreement, quotation, order form, statement of work, or other applicable agreement.

---

1. Scope of this Privacy Policy

This Privacy Policy applies to personal information processed through:

a. PayrollPRO websites, landing pages, contact forms, inquiry forms, demo request forms, and marketing pages;
b. PayrollPRO HRIS, employee records, 201 files, document management, policies, announcements, onboarding, offboarding, performance, ticketing, and employee servicing tools;
c. PayrollPRO timekeeping, attendance, web time tracker, biometric integration, DeviceHub, schedules, leaves, overtime, rest day, holiday, night differential, and attendance dispute features;
d. PayrollPRO payroll, payroll reports, payslips, payroll register, deductions, benefits, allowances, final pay, government reporting, and statutory contribution features;
e. PayrollPRO support, training, deployment, implementation, system calibration, data migration, troubleshooting, and account management;
f. PayrollPRO managed payroll, outsourced payroll, employer-of-record support, lodgment services, and related professional services, where applicable; and

g. communications through email, chat, messaging apps, calls, social media pages, and other authorized support channels.

This Privacy Policy does not replace the privacy policy of the Client/employer. For employee records, payroll records, attendance data, and HR data uploaded or processed under a Client account, the Client/employer remains primarily responsible for informing employees and securing the necessary legal basis, notices, authority, and approvals for processing.

---

2. Definitions

For purposes of this Privacy Policy:

Client means the company, employer, organization, partner, or subscriber that contracts with PayrollPRO or uses PayrollPRO for HR, timekeeping, payroll, employee records, government reporting, or related services.

Employee means an employee, worker, consultant, contractor, applicant, former employee, or member whose information is uploaded, entered, processed, or managed by a Client through PayrollPRO.

Company Admin means a person authorized by a Client to manage the Client account, users, access rights, employee data, payroll settings, timekeeping rules, approvals, reports, configurations, and related system functions.

User means any person who accesses or uses PayrollPRO, including Clients, Company Admins, Employees, support users, authorized representatives, or other registered users.

Personal Information refers to any information from which the identity of an individual is apparent or can be reasonably and directly ascertained, or which, when combined with other information, would directly and certainly identify an individual.

Sensitive Personal Information includes information classified as sensitive under applicable law, such as government-issued identifiers, tax identification details, health-related records where applicable, payroll/bank details, biometric information, and other legally protected information.

Processing includes collection, recording, storage, organization, updating, retrieval, use, consolidation, blocking, erasure, disclosure, transfer, or destruction of personal information.

---

3. Our Role in Processing Personal Data

PayrollPRO may act in different capacities depending on the activity:

3.1 PayrollPRO as Personal Information Controller

PayrollPRO acts as a Personal Information Controller for personal data that we collect and determine the purpose and means of processing, such as:

a. website inquiries;
b. demo requests;
c. marketing subscriptions;
d. client contact persons;
e. billing and account records;
f. support communications;
g. vendor, partner, and business development records;
h. PayrollPRO user account administration; and
i. internal compliance, accounting, legal, and security records.

3.2 PayrollPRO as Personal Information Processor

PayrollPRO generally acts as a Personal Information Processor for employee, HR, attendance, timekeeping, payroll, biometric, government reporting, and other employment-related data processed on behalf of a Client.

In this role, PayrollPRO processes personal data based on the Client's instructions, subscribed package, service agreement, order form, system configuration, support request, data processing agreement, or other written instruction.

The Client remains responsible for ensuring that the personal data uploaded or processed through PayrollPRO was collected lawfully, is accurate, is necessary for the intended HR/payroll purpose, and is supported by appropriate notice, consent, contract, legal obligation, legitimate interest, or other lawful basis.

---

4. Personal Information We Collect

Depending on your role, subscribed package, and use of PayrollPRO, we may collect and process the following categories of information:

4.1 Website and Inquiry Information

a. name;
b. company name;
c. job title or role;
d. email address;
e. mobile number or telephone number;
f. message, inquiry, or request details;
g. preferred meeting schedule;
h. source of inquiry; and
i. communication history.

4.2 Account and User Information

a. name;
b. email address;
c. username or user ID;
d. role, permission level, access rights, and assigned company;
e. login history;
f. password credentials in encrypted or hashed form, where applicable;
g. system activity logs;
h. support tickets and communications; and
i. user preferences and notification settings.

4.3 Employee and HRIS Information

Where a Client uses PayrollPRO for HRIS or employee records, the platform may process:

a. employee number;
b. name;
c. address and contact information;
d. date of birth, civil status, gender, nationality, and other profile information where required by the employer;
e. employment status, position, department, branch, cost center, team, supervisor, and reporting line;
f. employment start date, separation date, work assignment, contract details, and employment records;
g. 201 files, contracts, IDs, certificates, forms, attachments, and documents uploaded by the Client or User;
h. benefits, compensation package, leave credits, and work schedule details; and
i. other employment-related data required by the Client.

4.4 Timekeeping, Attendance, and Device Data

Where applicable, PayrollPRO may process:

a. time-in and time-out records;
b. web tracker logs;
c. mobile attendance logs;
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, face/photo capture logs, card reader, or device logs, 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 trail; and
i. device connection logs and technical metadata.

PayrollPRO does not require Clients to use biometric devices unless such integration is part of the subscribed package or approved implementation scope.

4.5 Payroll and Statutory Information

Where PayrollPRO is used for payroll, managed payroll, or government reporting, we may process:

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

4.6 Recruitment, Onboarding, Offboarding, and Performance Data

Where subscribed or enabled, PayrollPRO may process applicant, candidate, onboarding, offboarding, clearance, performance evaluation, KPI, survey, feedback, policy acknowledgement, training, career development, and related HR data.

4.7 Technical, Log, and Usage Information

When you access our website or platform, we may collect:

a. IP address;
b. browser type;
c. device type;
d. operating system;
e. pages visited;
f. referring and exit pages;
g. date and time of access;
h. session identifiers;
i. cookies and similar technologies;
j. system logs, audit logs, error logs, and security logs; and
k. usage activity needed for support, security, analytics, and platform improvement.

---

5. How We Collect Information

We collect personal information through:

a. information submitted directly by Clients, Company Admins, Employees, and Users;
b. employee masterlist uploads, HRIS records, payroll templates, forms, attachments, and

migration files;
c. information generated by the use of PayrollPRO modules;
d. biometric devices, DeviceHub, attendance systems, APIs, integrations, or connected devices, where applicable;
e. website forms, demo requests, email inquiries, social media pages, chat, calls, and support channels;
f. cookies, analytics, logs, and similar technologies;
g. authorized third-party service providers and integration partners; and
h. public or business sources used for legitimate business contact, sales, partnership, or support purposes.

---

6. Purposes of Processing

We process personal information for the following purposes:

6.1 To Provide PayrollPRO Services

a. create and administer accounts;
b. provide access to subscribed modules;
c. process HRIS, employee records, timekeeping, attendance, payroll, payslip, government report, ticketing, onboarding, offboarding, final pay, and related functions;
d. configure company rules, workflows, roles, schedules, pay codes, payroll settings, and reports;
e. support system deployment, migration, testing, parallel run, go-live, and stabilization;
f. provide client support, troubleshooting, and technical assistance; and
g. maintain audit trails, system logs, and accountability records.

6.2 To Support Payroll and HR Compliance

Subject to the Client's instructions and subscribed services, we may process data to support:

a. payroll computation;
b. attendance and timekeeping summary;
c. employee benefits and deductions;
d. statutory contribution reports;
e. tax-related payroll summaries;
f. government report generation;
g. final pay computation support; and
h. payroll-related documentation.

PayrollPRO does not provide legal, tax, or labor advice unless separately agreed in writing. Clients remain responsible for reviewing and validating payroll outputs, employment policies, attendance rules, tax treatment, benefits, and statutory submissions.

6.3 To Maintain Security and Platform Integrity

a. authenticate users;
b. manage access controls;
c. prevent unauthorized access;
d. detect, investigate, and prevent fraud, abuse, misuse, malware, security incidents, or illegal activity;
e. maintain logs and backups;
f. enforce Terms of Use and service agreements; and
g. protect PayrollPRO, Clients, Employees, Users, and the public.

6.4 To Communicate With You

a. respond to inquiries;
b. send service notices, administrative messages, security alerts, and support updates;
c. coordinate deployment, meetings, training, support, billing, and account matters;
d. send product updates, newsletters, offers, or business communications, subject to your opt-out rights; and
e. request feedback, conduct surveys, or improve client experience.

6.5 To Improve PayrollPRO

a. analyze platform usage;
b. improve system performance;
c. develop new features;
d. test, debug, and enhance product functionality;
e. generate anonymized or aggregated insights; and
f. improve security, documentation, support, and user experience.

Where possible, we use aggregated, anonymized, or de-identified information for analytics and product improvement.

---

7. Legal Bases for Processing

Depending on the situation, PayrollPRO processes personal information based on one or more of the following:

a. consent;
b. performance of a contract;
c. compliance with legal or regulatory obligations;
d. legitimate business interest, provided that such interest does not override the rights and freedoms of the data subject;
e. protection of lawful rights and interests in legal claims, audits, investigations, or dispute resolution;
f. fulfillment of the Client's employment, payroll, HR, accounting, tax, statutory, or operational requirements; and
g. other lawful grounds under applicable data protection laws.

For Employee data, the Client/employer is primarily responsible for determining and documenting the lawful basis for collection and processing.

---

8. Sharing and Disclosure of Information

We do not sell personal information.

We may share or disclose personal information only when necessary and lawful, including the following:

8.1 Within the Client Account

Information entered or generated under a Client account may be accessible to authorized Company Admins, HR users, payroll users, managers, approvers, employees, support users, and other authorized roles based on the Client's access configuration.

8.2 Service Providers and Subprocessors

We may engage reputable service providers, vendors, contractors, hosting providers, cloud infrastructure providers, communication tools, analytics providers, payment processors, support tools, security tools, and integration providers to help operate PayrollPRO.

Such parties may process personal information only as needed to provide their services and subject to confidentiality, security, and data protection obligations.

8.3 Government, Regulatory, Legal, or Lawful Requests

We may disclose information when required or permitted by law, court order, subpoena, lawful government request, audit, investigation, regulatory requirement, or to protect our rights, property, users, clients, employees, systems, or the public.

8.4 Business Transfers

If PayrollPRO or ADI undergoes a merger, acquisition, reorganization, financing, asset transfer, or similar business transaction, personal information may be transferred as part of that transaction, subject to appropriate safeguards and applicable law.

8.5 With Consent or Instruction

We may share information with third parties when authorized by the Client, User, data subject, contract, order form, statement of work, service request, or other lawful instruction.

---

9. Client and Company Admin Responsibilities

Clients and Company Admins are responsible for:

a. ensuring that employee, applicant, contractor, consultant, and user data uploaded to PayrollPRO is lawfully collected and accurate;
b. providing proper privacy notices to employees and other data subjects;
c. securing necessary consents, authorizations, or lawful bases where required;
d. managing user access, roles, passwords, permissions, approvers, and administrator privileges;
e. ensuring that only authorized personnel access payroll, HR, attendance, biometric, and employee data;
f. validating payroll, attendance, government reports, payslips, final pay, and related outputs before use or release;
g. promptly informing PayrollPRO of changes that may affect payroll calculations, security, privacy, or access control;
h. maintaining their own backups and downloaded copies of critical payroll and HR reports, where appropriate;
i. complying with labor, tax, payroll, accounting, government, employment, and data privacy laws; and
j. preventing misuse, unauthorized disclosure, credential sharing, or unlawful use of PayrollPRO.

PayrollPRO is not responsible for errors, privacy issues, payroll issues, or unauthorized access caused by incomplete or incorrect client data, client-side misconfiguration, unauthorized user activity, shared passwords, delayed approvals, undocumented policies, or failure of the Client to validate outputs.

---

10. Cookies and Similar Technologies

PayrollPRO websites and platforms may use cookies, analytics tools, session technologies, and similar tracking technologies to:

a. keep users logged in;
b. remember preferences;
c. secure sessions;
d. analyze website and platform usage;
e. improve performance;
f. detect abuse or suspicious activity; and
g. support marketing and communication activities.

Users may control cookies through browser settings. Disabling cookies may affect website or platform functionality.

Where third-party analytics or advertising tools are used, such tools may collect information subject to their own privacy policies, unless governed by PayrollPRO’s contractual arrangements.

---

11. Payment Information

Where online payments are made available, payment information may be processed by third-party payment processors. PayrollPRO does not intend to store full credit card information unless expressly required and protected under appropriate security standards.

Payment processors are responsible for their own payment processing systems, security, and compliance practices.

---

12. Data Ownership

As between PayrollPRO and the Client, employee records, payroll data, attendance data, HRIS records, reports, uploaded files, and other Client-provided or Client-generated operational data remain owned by the Client, subject to the applicable agreement.

PayrollPRO retains ownership of its platform, system design, source code, database structure, workflows, templates, reports, documentation, business logic, user interface, brand, intellectual property, and platform improvements.

PayrollPRO may retain copies of records as necessary for:

a. legal compliance;
b. tax, accounting, audit, and professional record keeping;
c. security logs and evidence;
d. dispute resolution;
e. enforcement of agreements;
f. backup and disaster recovery; and
g. legitimate business continuity purposes.

---

13. Data Retention

We retain personal information only for as long as reasonably necessary for the purpose for which it was collected, or as required by law, contract, accounting, audit, tax, employment, security, legitimate business, or dispute-resolution purposes.

For Client-controlled employee and payroll data, retention may depend on:

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

g. backup cycles; and
h. applicable service agreement, DPA, or order form.

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

a. allow the Client to export or download available data;
b. return data in a reasonable format;
c. delete or anonymize data after the applicable retention period;
d. retain limited archival, backup, audit, legal, or compliance records; and
e. suspend or remove access after termination or non-payment.

Some records, such as payroll history, audit logs, statutory reports, accounting records, and security logs, may not be immediately deletable if retention is required for legal, audit, accounting, payroll, or dispute-resolution purposes.

---

14. Data Security

PayrollPRO implements reasonable and appropriate technical, organizational, and administrative safeguards designed to protect personal information against unauthorized access, use, disclosure, alteration, loss, misuse, or destruction.

These safeguards may include:

a. access controls and role-based permissions;
b. authentication and password protection;
c. encrypted transmission where supported;
d. secure hosting and server controls;
e. data backups and recovery processes;
f. audit logs and activity logs;
g. system monitoring and troubleshooting controls;
h. confidentiality obligations for personnel, contractors, and service providers;
i. restricted access to payroll, employee, HR, and sensitive data; and
j. security reviews and system maintenance.

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

---

15. Security Incidents and Data Breach Notification

If PayrollPRO becomes aware of a security incident or personal data breach involving personal information processed by PayrollPRO, we will take reasonable steps to:

a. investigate and contain the incident;
b. assess the nature, scope, and potential impact;
c. preserve relevant evidence and logs;
d. notify affected Clients where required or appropriate;
e. support the Client in complying with applicable data breach notification obligations; and
f. notify regulators or affected individuals where PayrollPRO is legally required to do so.

For employee or Client-controlled data, PayrollPRO may coordinate breach notification through the Client, unless direct notification is required by law or contract.

Clients must promptly notify PayrollPRO of any suspected unauthorized access, compromised credentials, incorrect disclosure, or security incident involving their account, users, devices, integrations, or data.

---

16. International Data Transfers

PayrollPRO may store, process, host, support, or transfer personal information in the Philippines or in other countries where our infrastructure, service providers, support providers, or authorized partners operate.

Where personal information is transferred internationally, PayrollPRO will take reasonable steps to ensure that such transfers are protected through appropriate contractual, organizational, and technical safeguards, and are handled in accordance with applicable data protection requirements.

Clients should inform PayrollPRO if they require specific data residency, localization, or cross-border transfer terms, so these can be addressed in the service agreement, DPA, order form, or implementation scope.

---

17. Employee Requests and Data Subject Rights

Under applicable data protection laws, data subjects may have rights such as:

a. the right to be informed;
b. the right to access personal information;
c. the right to correct inaccurate or outdated information;
d. the right to object to processing;
e. the right to erasure or blocking in proper cases;
f. the right to data portability, where applicable;
g. the right to damages where legally available; and
h. the right to file a complaint with the appropriate data protection authority.

If you are an Employee, applicant, consultant, contractor, or former employee of a PayrollPRO Client, please direct requests relating to your employment, HR, attendance, payroll, benefits, government records, or 201 file to your employer or Client’s authorized

HR/Admin team. PayrollPRO may not be able to directly modify, release, delete, or correct Client-controlled employee data without the Client's instruction or authorization.

If PayrollPRO controls the data involved, such as website inquiries, marketing subscriptions, or PayrollPRO account contact information, you may contact us using the details below.

We may need to verify your identity and authority before acting on a request.

---

18. Marketing Communications

We may send business, product, service, newsletter, event, update, or promotional communications to Clients, prospects, partners, and users where allowed by law.

You may opt out of marketing emails by using the unsubscribe link, changing your preferences, or contacting us. Even if you opt out of marketing communications, we may still send service-related messages, administrative notices, security alerts, billing notices, and support communications.

---

19. Public Posts, Testimonials, and Feedback

If you submit a testimonial, review, public comment, social media post, forum post, or similar content, we may display it with your name, company, role, or other details you provided, subject to your consent or applicable permission.

If you want your testimonial or public reference removed, you may contact us. We will review and act on the request where reasonably possible.

---

20. Children's Privacy

PayrollPRO is intended for business, employer, HR, payroll, and workforce management use. It is not intended for children or minors as direct users.

If a Client processes minor-related employment, internship, training, or dependent information through PayrollPRO, the Client is responsible for ensuring that such processing is lawful, necessary, properly authorized, and compliant with applicable laws.

---

21. Third-Party Links and Integrations

PayrollPRO may contain links, integrations, APIs, embedded tools, device connections, payment processors, government portals, biometric devices, accounting systems, HR systems, or other third-party services.

We are not responsible for the privacy practices, security, content, or policies of third-party websites, portals, systems, or devices that are not controlled by PayrollPRO. Clients and Users should review the privacy and security policies of such third parties.

---

22. Changes to this Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our services, technology, legal requirements, operations, or privacy practices.

If we make material changes, we may notify Clients or Users through email, platform notice, website notice, contract update, or other reasonable means.

The updated Privacy Policy will be effective on the date posted or on the date stated in the notice.

---

23. Contact Us

For privacy questions, data subject requests, security concerns, or requests for more information, you may contact:

Analytics and Data Integrity, Inc. / PayrollPRO
Data Protection Officer / Privacy Officer: [Insert Name / Designation]
Email: support@payrollpro.ph
Alternative Email: support@adiconsulting.ph
Office Address: Unit 323, Vinia Building, 929 Epifanio de los Santos Ave., Philam, Quezon City, Metro Manila, Philippines
Website: https://payrollpro.ph

For employee, attendance, payroll, HR, or company record concerns, Employees should first contact their employer's HR, Payroll, or Company Admin team.

Recommended Add-On Documents

For stronger compliance, PayrollPRO should also maintain:

1. **Annex B – Data Processing Agreement** for Clients
2. **Cookie Policy**
3. **Subprocessor List**

4. **Data Retention and Deletion Policy**
5. **Information Security Policy**
6. **Data Breach Response Procedure**
7. **Employee Data Subject Request Procedure**
8. **Biometric / DeviceHub Privacy Notice** for clients using biometric attendance devices.