Data Privacy & Protection Policy

EaziWage

Data Privacy & Protection Policy

Version History

Version No.	Date Updated	Updated By	Update Summary
1	17 Oct 2025	Jason Crawford	First DPP Policy

Approval Record

Version No.	Date Approved	Approved By
1	17 Oct 2025	EaziWage Holdings Limited Board Members

Ownership

Chief Executive Officer

Applicability

The Data Privacy & Protection ("DPP") Policy ("the Policy") applies to all employees, employers, contractors, agents, investors, banks and any other individuals or entities within the EaziWage Group, if and where relevant.

Failure to comply with these policies and procedures may result in disciplinary action, including but not limited to warnings, additional training, termination of employment, or legal action.

1. Data Privacy & Protection Policy Purpose and Scope

This Policy sets out how EaziWage Holdings Limited ("EaziWage", the "Firm", "we/us/our") and its associated entities (the "Group") collects, uses, discloses, transfers, stores, and protects personal data when providing earned-wage access and related services (the "Services"). It applies to: (i) employees/end-users, (ii) employer clients/HR & payroll admins, (iii) prospective users, (iv) our own staff, and (v) vendors and other "associated persons".

We are a **data controller** when we determine the purpose and means of processing (e.g., onboarding, KYC, credit/disbursement rails where applicable). Some activities may involve **data processor** roles (e.g., where we purely host or process on documented instructions of an employer). We will register with the **Office of the Data Protection Commissioner (ODPC)** as required under the **Data Protection Act No. 24 of 2019 (DPA)** and Registration Regulations.

2. Legal & Regulatory Framework

We comply with:

- **Data Protection Act of 2019 (No. 24 of 2019)**
- **Data Protection (General) Regulations of 2021** (the "General Regulations").
- **Data Protection (Registration of Data Controllers and Data Processors) Regulations of 2021**.
- **ODPC Guidance** including DPIA guidance and data-sharing code drafts.

Where applicable, sectoral obligations (e.g., CBK rules via regulated partners) and AML/CFT obligations will also apply.

3. What Data We Collect

A. Identification & contact: Full name, national ID/passport no., KRA PIN (where relevant), mobile number, email, address.

B. Employment & payroll: Employer name, staff ID, department, employment status, salary band, net/gross pay, pay cycle, leave/attendance (if used to compute earned wages).

C. Financial/payment: Employee bank or mobile-money details (e.g., pay-out account), employer funding/settlement accounts, transaction identifiers, timestamps, amounts, fees.

D. Technical & app usage: Device identifiers, IP, app telemetry, cookies/SDK events/

E. Verification/KYC artifacts: Documents/photos strictly for verification where required.

F. Support & comms: Tickets, call recordings (where lawful), consents, preferences.

G. Special categories (sensitive personal data): Under the DPA, sensitive personal data includes (among others) health, biometric, genetic, ethnicity, sexual life, family details, spending habits and property details. We minimise collection of any sensitive data and apply heightened safeguards and lawful-basis checks when it is unavoidable (e.g., property or family details embedded in employer HR files).

4. Lawful Bases for Processing

Depending on the context, we rely on one or more of the following lawful bases:

- **Contract performance** – to provide the EWA service requested by the employee or employer;
- **Legal obligation** – to meet financial-crime, tax, employment, or data-protection obligations;
- **Legitimate interests** – to run, secure, and improve our platform (balanced against your rights);
- **Consent** – for specific optional features (e.g., marketing, certain analytics, or where consent is required for cross-border transfers of **sensitive personal data**).

For **sensitive personal data**, we ensure an additional condition is met under the DPA before processing.

5. Purpose Limitation & Data Minimisation

We collect only what is necessary for: (i) verifying identity and employment; (ii) calculating earned-wage eligibility; (iii) disbursing funds; (iv) reconciliation, settlement, audit, and AML; (v) customer support; (vi) product improvement & security; and (vii) legal and regulatory compliance. We do not use data for unrelated purposes without a compatible lawful basis and (where required) fresh consent.

6. Data Subject Rights

Under Kenyan law, you have the right to: **be informed, access, rectify/correct, object/restrict, data portability (where technically feasible),** and **erasure** (subject to legal/contractual limits).

Requests are handled within statutory timelines and recorded where identity verification is required.

7. Children's Data

EaziWage is intended for adults in employment. We do not knowingly onboard children. If children's data appears in HR files (e.g., dependants for benefits), we process strictly under the DPA's heightened safeguards and only as required by the employer's lawful purpose.

8. Data Sharing & Processors

We may share data strictly on a **need-to-know** basis with:

- **Payment partners and banks/investors** for pay-outs and settlement;
- **Employers** (limited reports necessary to operate EWA and reconcile deductions);
- **Regulated financial-crime partners** (e.g., sanctions screening/KYC where applicable);
- **Vendors/IT processors** (hosting, SMS/OTP, support tools) under written DPAs;
- **Authorities/regulators** when required by law or valid legal process.

Routine data sharing requires **data-sharing agreements** and documented governance per ODPC guidance and the General Regulations.

We prohibit "onward sharing" by third parties without our written authorisation and equivalent safeguards.

9. International (Cross-Border) Transfers

Personal data may be transferred outside Kenya only under the DPA and General Regulations, including:

- **Adequacy** or **appropriate safeguards** (e.g., SCCs/BCRs) demonstrated to ODPC;
- **Necessity** exceptions defined in law; and
- **Consent** for transfers of **sensitive personal data** where required. We document transfer risk assessments and safeguards.

10. Retention & Deletion

We retain personal data **no longer than necessary** for the purposes above, taking into account statutory retention (e.g., AML/audit, employment law, tax). We maintain a retention schedule; when the period expires, data is securely deleted or anonymised, except where legal holds apply.

11. Cookies, SDKs & Similar Tech

Our app/website may use cookies and mobile SDKs for **security (fraud/abuse prevention)**, **core functionality**, and **analytics**. Where required, we obtain consent and provide granular controls. You can manage settings in-app or via browser options. See our Cookie/SDK Notice for details on vendors, purposes, and retention.

12. Security Safeguards

We implement technical and organisational measures proportionate to risk, including: encryption in transit/at rest; network segmentation; device attestation; secrets management; role-based access and least privilege; secure SDLC; vendor security due

diligence; continuous monitoring; and incident response with evidenced runbooks. We test controls regularly and train staff.

13. Breach Notification

If a personal-data breach occurs, we will assess impact and notify the **ODPC within 72 hours of becoming aware** where the breach meets notification thresholds, and notify affected data subjects **without undue delay**, consistent with the DPA/General Regulations and ODPC practice. We maintain breach logs and cooperation with the ODPC.

14. Data Protection Impact Assessments (DPIA)

Given the scale and sensitivity of payroll/financial processing, we conduct a **DPIA** prior to launch and whenever we introduce major changes (e.g., new data sources, profiling logic, or cross-border transfers). The DPIA documents risks, mitigations, and residual risk acceptance, following ODPC Guidance.

15. Registration & Records of Processing

We maintain an up-to-date **Record of Processing Activities** (ROPAs), consents, DPIAs, data-sharing agreements, vendor DPAs, and breach registers. We register with the ODPC as a **data controller/processor** as applicable and keep registrations current (noting small-entity exemptions do not generally apply to firms processing payroll/financial data at scale).

16. Automated Decision-Making & Profiling

Where we use automated rules (e.g., to estimate earned-wage eligibility or apply fraud controls), we ensure fairness, transparency, and human review on request. We avoid solely automated decisions that produce **legal or similarly significant effects** without appropriate safeguards. You may request an explanation and contest such decisions.

17. Your Choices

- **Access & correction:** Request copies or corrections of your data.
- **Deletion:** Request deletion where we have no lawful need to keep it.
- **Objection/Restriction:** Object to certain processing or ask us to pause it (e.g., marketing).
- **Portability:** Request machine-readable copies where technically feasible. We will explain any lawful or contractual limits to these rights.

18. Contact, Complaints & ODPC

Data Protection Officer (DPO)/Privacy Office
EaziWage Holdings Limited
Email: **privacy@eaziwage.com**

If you believe your data has been mishandled, contact us first. You may also complain to the **Office of the Data Protection Commissioner (ODPC)** via official channels.

19. Changes to this Policy

We review this Policy at least **annually** or upon material changes (law, guidance, features, vendors, transfers). We will notify users in-app/email for material updates and maintain a change log.

Contact Us

info@eaziwage.com

+254 72 315 4900

EaziWage