K I P L E P E O P L E

Privacy Policy

Kiple People's HR Platform (Mobile App & Web Portal)

Version 0.1 · Last Updated: 24 July 2026· Kiplepay Sdn Bhd

Contents

1. Introduction 3
2. Glossary 3
3. Scope of this Policy 3
4. Who Controls Your Data 4
5. Personal Data We Collect 4
6. How We Collect Your Personal Data 6
7. Purposes of Collection, Use and Disclosure of Personal Data 6
8. Legal Basis for Processing 6
9. Disclosure of Personal Data 8
10. Data Security 8
11. Data Breach Notification 9
12. Data Retention 9
13. Your Rights & How to Exercise Them 10
14. Cookies, Web Beacons, and Diagnostic Data 10
15. Third-Party Sites and Services 11
16. Cross-Border Data Transfer 11
17. Relationship with the KiplePay App 11
18. Changes to This Policy 11
19. Language 11
20. Complaints 11
21. Contact Us 11

1. Introduction

Green Packet Berhad and its relevant subsidiaries and affiliates, including the entity operating the Kiple People platform ("Kiple People", "we", "us", or "our"), respect your privacy and take our obligations under Malaysia's Personal Data Protection Act 2010 ("PDPA") seriously.

This Privacy Policy explains how we collect, use, disclose, and process the Personal Data you provide in the course of using the Kiple People mobile application and web portal, and any related functionalities, services, or features offered in connection with them (collectively, the "Platform"), made available to you through your employer ("Employer", "Company", "Customer").

By registering for, communicating with us through, or otherwise using the Platform, you acknowledge that you have read and understood this Policy, and you agree and expressly consent to the collection, use, processing, disclosure, and transfer of your Personal Data and Sensitive Personal Data as described in this Policy.

As a service provider to your Employer, Kiple People collects and processes Personal Data primarily according to our Employer-customer's instructions and requirements. If you have questions about your Employer's specific HR policies, or wish to exercise rights over data your Employer controls, you should first refer to your Employer's own privacy policy or contact your Employer's HR department.

2. Glossary

"Affiliate" means any company or entity controlling, controlled by, or under common control with Green Packet Berhad. "Control" means ownership of 50% or more of the voting equity of an entity.

"Authorised Third Party" means business partners, contractors, agents, auditors, advisers, payment gateway providers, banking partners, cloud hosting providers, the eKYC verification provider, and the Earned Wage Access (EWA) service provider, engaged by us from time to time to help provide the Platform to you.

"eKYC" means the electronic Know-Your-Customer identity verification process required to activate the e-Wallet feature.

"e-Wallet" means the internal digital wallet feature within the Platform. It is separate and distinct from the Kiple E-Wallet / KiplePay consumer application operated by Kiplepay Sdn Bhd.

"Employer" means the company that has subscribed to Kiple People's services and through which your access to the Platform is provided.

"EWA" means Earned Wage Access, the feature allowing withdrawal of earned but unpaid salary prior to the standard payroll date.

"Personal Data" shall have the same meaning given to it under the PDPA broadly, any information relating directly or indirectly to you that is capable of identifying you.

"Platform" means collectively the Kiple People mobile application, web portal, and any related services, features, or functionalities made available by us from time to time.

"Sensitive Personal Data" shall have the same meaning given to it under the PDPA, and includes (without limitation) data relating to physical or mental health, religious beliefs, the commission or alleged commission of an offence, and biometric data.

"Statutory Bodies" refers to the Employees Provident Fund (EPF/KWSP), the Social Security Organisation (SOCSO/PERKESO), the Inland Revenue Board of Malaysia (LHDN), and HRD Corp.

"you, your, User" means you, the employee accessing and/or using the Platform.

3. Scope of this Policy

This Policy applies to you from the moment you register for, access, or use the Platform. This Policy forms part of, and should be read together with, the Terms and Conditions governing your use of the Platform.

Kiple People has no direct relationship with individuals whose Personal Data is provided to us by an Employer for the purpose of using the Platform, beyond the Platform account itself. If you are or were employed by a

company using the Platform, and you seek to access, correct, object to the processing of, or delete your Personal Data, and you are unable to do so via your own account access, you should direct your request to your Employer's HR department in the first instance, who administers the Platform for your organisation.

4. Who Controls Your Data

Two parties are generally involved in handling your Personal Data on the Platform:

- Your Employer is generally the "Data Controller" for HR-related data (such as your salary, leave records, and claim history) since your Employer determines what data is collected and for what purposes, and instructs Kiple People accordingly.
- Kiple People acts as a "Data Processor" providing the technology platform on your Employer's behalf, and additionally acts as a "Data Controller" in its own right for data relating to the e-Wallet, eKYC verification, and EWA features, which are provided as regulated or quasi-regulated financial services layered on top of the core HR platform.

5. Personal Data We Collect

5.1 Information You Provide Directly

- Account information: full name, email address, phone number, employee ID, job title, department, country.
- Identity verification (eKYC) information: MyKad/NRIC number and images (front and back), passport details (for non-citizens), and a facial image/selfie captured during the liveness check.
- Leave and claims information: leave applications, reasons for leave, medical certificates or other supporting documents you upload, expense claim details and receipts.
- Financial information: bank account details (for claim payouts and wallet-to-bank transfers), transaction history within the e-Wallet.
- Communications: any information you provide when contacting HR or support through the Platform.

5.2 Information We Collect or Process on Behalf of Your Employer

As a service provider, Kiple People collects and processes the following categories of Personal Data on behalf of, and per the instructions of, your Employer, generally when your Employer or its HR Admin enters, or you yourself enter, such data into the Platform:

- Name, date of birth, gender, contact details, emergency contact details, address, nationality, race, ethnic origin, qualifications, education, occupation, employer, former employer(s).
- Income range, salary and bank account details, income tax file number, Form EA and other tax records, EPF (KWSP) statements and information, SOCSO/EIS records, HRDF records.
- Photographs or other images, facial recognition data, fingerprint or other biometric data, location data, family member details, and national identification number, where these are collected for eKYC, attendance, or payroll purposes as instructed by your Employer.
- For attendance and payroll purposes specifically: face images, GPS location (during active Work-From-Home clock-in/out sessions only, where enabled), IP address, unique device identifiers, leave details, bank account details, and tax declarations.

5.3 Information Collected Automatically

- Device information: device type, operating system, unique device identifiers, IP address.
- Usage information: log-in times, features accessed, app performance and crash data, click-stream information.
- Cookies and similar technologies used on the web portal, see Section 14.

5.4 Sensitive Personal Data

The following Sensitive Personal Data may be collected and/or processed solely for the purpose of providing the Platform's services:

- Physical or mental health data, such as details on a medical certificate submitted with a leave application.
- Biometric data, such as facial recognition data and fingerprint data, used for eKYC identity verification and/or attendance tracking, where these features are enabled by your Employer.

By using the Platform, you explicitly consent to our collection and processing of your Sensitive Personal Data for these purposes.

5.5 Personal Data of Minors

The Platform is intended for use by working adults and is not directed at children. We do not knowingly collect Personal Data from individuals under the age of 18 without the consent of a parent or legal guardian. If you are under the age of 18, you must obtain consent from your parent(s) or legal guardian before providing any Personal Data to us. If you are the Employer, and you provide or disclose the Personal Data of any employee under the age of 18 (for example, a legitimate intern or apprentice), you warrant and represent that the express consent of that individual's parent(s) or legal guardian(s) has been obtained prior to such disclosure to us.

5.6 Personal Data of Third Parties

If you submit or disclose the Personal Data of any third party through the Platform (for example, emergency contact details or family member details), you represent and warrant that you have obtained that third party's consent for us to collect, transfer, and process their Personal Data in accordance with this Policy.

6. How We Collect Your Personal Data

Generally, we collect Personal Data in the following ways:

- When you register for and set up your Platform account.
- When your Employer's HR Admin enters or uploads your employee record, salary information, or leave entitlements into the Platform.
- When you submit a leave application, expense claim, or eKYC verification through the Platform.
- When you use the e-Wallet or EWA features, or perform a transaction through the Platform.
- When the Platform captures face images, biometric data, or location details for the purpose of calculating attendance, payroll, or verifying your identity, where these features are enabled by your Employer.
- When you interact with our customer support or HR support functions, including through in-app messaging, email, or phone.
- When you enter Personal Data into any digital form on the Platform.

7. Purposes of Collection, Use and Disclosure of Personal Data

Subject to applicable law, we may collect, use, and disclose your Personal Data for the following purposes:

- To create and manage your Platform account and authenticate your identity.
- To process leave applications, approvals, and maintain accurate leave balance records.
- To process expense claims, route them through the applicable approval tier, and disburse approved payouts (via e-Wallet or bank transfer).
- To calculate and process payroll, including statutory contributions (EPF, SOCSO, EIS, PCB), and to generate payslips and annual tax forms (Form EA).
- To verify your identity through eKYC and activate your e-Wallet.
- To process e-Wallet transactions (QR payments, bank transfers, peer-to-peer transfers) that you initiate.
- To process EWA withdrawal requests, where enabled by your Employer, including via our third-party EWA service provider where applicable.
- To calculate attendance, including via geo-location during active Work-From-Home clock-in/out sessions, where enabled by your Employer.
- To respond to your enquiries, feedback, requests, or complaints.
- For internal administrative purposes, record-keeping, and reporting to your Employer.
- To detect, investigate, and prevent fraud, unauthorised transactions, and security incidents.
- To comply with our legal and regulatory obligations, including reporting to Statutory Bodies and responding to lawful requests from authorities.
- To send you service-related notifications (e.g. leave approval status, claim status, wallet transaction alerts, payroll notices).
- For quality assurance, staff training, and identity verification purposes, including where phone calls with our support team are recorded.
- To improve the Platform's functionality, reliability, security, and user experience, including through research, testing, and statistical analysis conducted on an aggregate and/or anonymised basis.
- For any other purpose which we have specifically notified you of at or before the time your Personal Data is collected.

8. Legal Basis for Processing

We process your Personal Data on the following bases: (a) your consent, given at registration and at the point of completing eKYC and activating e-Wallet/EWA features; (b) performance of your employment relationship with your Employer and your Employer's contractual arrangement with Kiple People; (c) compliance with legal

obligations, including statutory payroll reporting; and (d) our legitimate interests in maintaining the security, integrity, and proper functioning of the Platform, provided this does not override your fundamental rights.

You may withdraw consent for optional features (such as e-Wallet or EWA) at any time, see Section 13 though you will no longer be able to use those specific features. You cannot withdraw consent for the processing of core HR data required for your employment relationship, as this is necessary for your Employer to meet its legal obligations.

9. Disclosure of Personal Data

We are not in the business of selling your Personal Data, and we will not sell or rent your Personal Data. We may, however, disclose your Personal Data to the following categories of recipients, for the purposes described in Section 7, who may be located in Malaysia or overseas:

9.1 Your Employer

Your HR Admin, your direct manager(s), and relevant approvers within your Employer's organisation have access to your HR-related data (leave, claims, payroll, approval status) as necessary to perform their roles. Your wallet PIN and raw eKYC biometric images are never visible to your Employer.

9.2 Statutory Bodies

As required by law, relevant payroll and statutory contribution data is reported to EPF (KWSP), SOCSO (PERKESO), the Inland Revenue Board (LHDN), and HRD Corp, where applicable.

9.3 Authorised Third Parties

- Payment gateway providers, to process prefund top-ups and wallet transactions.
- Banking partners, to process bank transfers and salary bank file submissions.
- Our third-party Earned Wage Access (EWA) provider [name to be confirmed], where your Employer has enabled the EWA feature via this third-party integration, prior to any in-house EWA solution being available.
- Our eKYC verification service provider, to process and verify your identity documents and biometric liveness check.
- Cloud hosting and data storage providers, who store Platform data on our behalf under contractual confidentiality and security obligations.
- Our Affiliates within the Green Packet / Kiple group of companies, where necessary to provide or support the Platform.

9.4 Business Transfers

If Green Packet Berhad or the Kiple People business is involved in a merger, acquisition, reorganisation, sale of assets, or similar corporate transaction, your Personal Data may be disclosed to the parties involved as part of that transaction, subject to appropriate confidentiality safeguards.

9.5 Legal and Regulatory Disclosure

We may disclose Personal Data where required by law, court order, or a valid request from a regulatory or law enforcement authority, including Bank Negara Malaysia in connection with e-money and payment services oversight.

10. Data Security

We implement technical and organisational measures designed to protect your Personal Data against unauthorised access, alteration, disclosure, or destruction, including:

- Encryption of data in transit and at rest.
- Access controls restricting Personal Data access to authorised personnel on a need-to-know basis, with role-based permissions.
- Your e-Wallet PIN is stored in hashed (encrypted, non-reversible) form and is never visible to Kiple People staff, your Employer, or any third party.
- Facial biometric data used for eKYC/attendance is stored securely; where face authentication is performed on your mobile device, the system verifies against locally stored data on your device before authenticating to the Platform.
- Multi-factor safeguards for wallet transactions (PIN verification, account lock after repeated failed attempts).

- Regular security assessments of the Platform infrastructure.

While we take reasonable steps to protect your data, no method of transmission or storage is completely secure, and we cannot guarantee absolute security. You also play a role in protecting your account by keeping your password and wallet PIN confidential.

11. Data Breach Notification

In the event of a security breach leading to accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of or access to Personal Data, we will promptly assess the impact. Where the breach is assessed to be a notifiable data breach under applicable law, we will report the breach to the relevant regulatory body or data protection authority within the timeframe prescribed by law. We will notify your Employer without undue delay upon establishing that a breach is likely to result in significant harm or impact to affected individuals, or is of a significant scale, so that your Employer can inform you as appropriate.

12. Data Retention

We retain your Personal Data for as long as necessary to fulfil the purposes outlined in this Policy, including:

- For the duration of your employment with your Employer, and for a period thereafter as required by applicable law (e.g. statutory record-keeping requirements under the Income Tax Act 1967 and Employment Act 1955, which may require retention of payroll records for a minimum of 7 years).
- eKYC verification records and wallet transaction records are retained in accordance with applicable AML/CFT and e-money regulatory record-keeping requirements.
- Facial biometric data used for eKYC or attendance is retained for as long as your Employer's account remains active. Where your Employer's account or your individual employment is terminated, associated facial biometric data will be removed from our active database within a reasonable period following termination (e.g. 30 days), subject to any longer retention required by law. Backup copies are deleted on a rolling schedule shortly after removal from the active database (e.g. within 7 days).

Upon expiry of the applicable retention period, your Personal Data will be securely deleted or anonymised, unless further retention is required by law.

13. Your Rights & How to Exercise Them

Subject to applicable exceptions under the PDPA, you have the right to:

- Request access to a copy of the Personal Data we hold about you, or information about how we use or disclose it.
- Request correction or updating of any Personal Data we hold about you which is inaccurate or incomplete.
- Request that we transmit your Personal Data to another data controller, subject to our technical feasibility and the compatibility of data formats.
- Withdraw your consent to the processing of your Personal Data for optional features (e.g. e-Wallet, EWA), subject to Section 8.
- Lodge a complaint with the Personal Data Protection Department of Malaysia if you believe your data has been mishandled.

To exercise these rights, submit your request in writing or by email to our Data Protection Officer using the contact details in Section 20. We will endeavour to respond to access and/or correction requests within 21 days of receipt.

Depending on the scope and nature of the work required to process your request, we may impose a reasonable fee to recover our administrative costs, and may require a deposit before processing. We will inform you of any applicable fee before processing your request.

If you are, or were, an employee of one of our Employer customers and you seek to exercise these rights over data provided to us by your Employer, and you are unable to do so via your Platform account access, you should direct your request to your Employer's HR department in the first instance, as your Employer controls the underlying HR data (see Section 4).

We may refuse to comply with a request where: you have not provided sufficient information to verify your identity or locate the relevant data; locating the specific data would impose a disproportionate burden or expense on us; providing access would result in the disclosure of a third party's Personal Data; or providing access would violate a court order, legal obligation, or duty of confidentiality.

Withdrawing your consent to the processing of your Personal Data does not affect our right to continue to collect, use, and disclose Personal Data where such processing without consent is permitted or required under applicable law. Depending on the nature of your request, withdrawing consent may mean we are no longer able to provide certain features of the Platform to you.

14. Cookies, Web Beacons, and Diagnostic Data

14.1 Cookies

The web portal may use cookies which are small text files placed in your browser or device to maintain your session, remember your preferences, and understand how the portal is used. Types of cookies used may include:

- Session cookies, which expire at the end of your browser session.
- Persistent cookies, which are stored on your device between browser sessions to remember your preferences.
- First-party cookies, set directly by the Platform.
- Third-party cookies, set by a third-party service integrated with the Platform, where applicable.

You may configure your browser to refuse cookies, though this may limit certain portal functionality, such as needing to log in more frequently.

14.2 Web Beacons and Similar Technologies

We may use web beacons (small graphic images, also known as "pixel tags") in conjunction with cookies to help understand usage patterns on the web portal.

14.3 Diagnostic and Usage Data

To help us improve the quality and performance of the mobile app, we may automatically collect diagnostic and usage information from your device, such as app crash details, which features you use and how often, your device type, and operating system version. This information is generally submitted to us without directly identifying you personally. Automatic reporting of diagnostic and usage information is typically enabled by default and can be reviewed in your device settings.

15. Third-Party Sites and Services

The Platform may contain links to, or integrate with, third-party applications, websites, or services (such as your bank's app, a payment gateway checkout page, or our EWA provider's service) to make certain functionality available to you. We are not responsible for the privacy practices or content of such third-party services. You should review the privacy policy of any third-party service before using it. This Policy applies only to Personal Data collected by us through the Platform.

16. Cross-Border Data Transfer

Your Personal Data is primarily stored and processed within Malaysia. Where any Personal Data is transferred to, stored in, or processed in a location outside Malaysia for example, by a cloud hosting provider, an Affiliate, or a third-party EWA provider located overseas, we will take reasonable steps to ensure such transfer complies with the requirements of the PDPA, including ensuring an adequate level of data protection at the receiving location. By continuing to use the Platform, you consent to such transfer where it occurs.

17. Relationship with the KiplePay App

The Kiple People e-Wallet described in this Policy is a feature built into the Kiple People Platform and is separate and distinct from the Kiple E-Wallet / KiplePay consumer mobile application, which is operated by Kiplepay Sdn Bhd and governed by its own separate Privacy Policy.

Where the Platform displays your KiplePay balance via API integration, or redirects you to install the KiplePay app, any Personal Data processed within the KiplePay app itself (as opposed to data displayed to you from within Kiple People) is governed by KiplePay's own Privacy Policy, available at KiplePay's website, and not by this Policy.

18. Changes to This Policy

We may amend this Policy from time to time, at our discretion, to ensure it remains consistent with our future developments, industry practice, and/or changes in legal or regulatory requirements. We will notify you of material changes through the Platform or via your Employer. Your continued use of the Platform after such changes take effect indicates your agreement to the revised Policy.

19. Language

If the Privacy Policy is translated into any other languages and there is a conflict between this English version and any foreign language version of this Privacy Policy, the English version shall prevail.

20. Complaints

If you have concerns about how your Personal Data has been handled, please first contact us using the details below. If you remain unsatisfied, you have the right to lodge a complaint with the Personal Data Protection Department of Malaysia (Jabatan Perlindungan Data Peribadi).

21. Contact Us

For questions, requests, or complaints regarding this Privacy Policy or your Personal Data, please contact:

Name:	Personal Data Officer
Address:	Kiplepay Sdn Bhd B-23A-3, The Ascent Paradigm Jalan SS7/26A, Kelana Jaya 47301 Petaling Jaya, Selangor, Malaysia
Phone number:	+60 3 2714 6288
Email:	support@kiplepay.com

Alternatively, you may contact your Employer's HR department for matters relating to your HR data specifically.

Kiple People - Privacy Policy

Kiplepay Sdn Bhd