Biller Privacy Policy

Last updated: 30 June 2026

This Privacy Policy explains how your personal data is collected, used, disclosed, stored and protected when you use the Biller mobile application (the "App") on Android and iOS, and the services offered through it. The App lets you buy digital, instant-delivery products only: prepaid mobile airtime and data top-ups for Malaysian telcos, and bill payments to utilities and similar billers. There are no physical goods and no shipping.

"Biller" is the trading name of Kira Labs Sdn Bhd for this App.

This Policy is issued under the Personal Data Protection Act 2010 (Act 709), as amended by the Personal Data Protection (Amendment) Act 2024 ("PDPA"), and forms part of the written notice required by section 7 of the PDPA. Please read it before you use the App or provide any personal data.

A Bahasa Malaysia version of this Policy is available at https://biller.my/legal/privacy-bm. If there is any inconsistency between the English and Bahasa Malaysia versions, the English version shall prevail.

1. Who we are: the data controller

The data controller responsible for your personal data is:

- **Kira Labs Sdn Bhd**, a company incorporated in Malaysia, trading as **"Biller"**
- Company registration number (SSM): 202601017340
- Registered address: 7-2, Plaza Danau 2, Jalan 2/109F, Taman Danau Desa, 58100 Kuala Lumpur, Wilayah Persekutuan Kuala Lumpur, Malaysia
- Support email: support@biller.my
- Support telephone: +60172208661

In this Policy, "Biller", "we", "us" and "our" refer to Kira Labs Sdn Bhd. "You" and "your" refer to the individual whose personal data we process, whether you use the App as a guest, a registered distributor or a registered dealer.

2. Data Protection Officer

We have appointed a Data Protection Officer ("DPO") who is accountable for our compliance with the PDPA. You may contact the DPO about this Policy, about how we handle your personal data, or to make a complaint or a request to exercise your rights:

- DPO name and title: Data Protection Officer, Kira Labs Sdn. Bhd.
- DPO email (dedicated and monitored): dpo@biller.my
- DPO business telephone: +60172208661
- DPO postal address: 7-2, Plaza Danau 2, Jalan 2/109F, Taman Danau Desa, 58100 Kuala Lumpur, Wilayah Persekutuan Kuala Lumpur, Malaysia

3. The personal data we collect

The personal data we collect depends on how you use the App. We collect only what we need for the purposes set out in Section 4.

3.1 Data we collect from everyone

Whether you use the App as a guest, a registered distributor or a registered dealer, we collect:

- **Device and anti-fraud signals**: an app-generated installation identifier (a random value created by the App and stored in secure storage on your device, not a hardware identifier and not an advertising identifier), device platform information, request correlation identifiers, and integrity/attestation tokens generated on your device (Google Play Integrity on Android and Apple App Attest on iOS). These are used to verify that requests come from a genuine app and device, to correlate your requests, and to prevent fraud and abuse. We do not use these to track you across other companies' apps or websites.
- **Push notification token** (if you allow notifications), together with the device platform, so we can send you transaction and service messages. The push token is collected for guest, distributor and dealer sessions.

3.2 Guest users (one-off purchases, no account)

When you buy as a guest, you do not create an account and you do not hold any stored balance. In addition to the data in Section 3.1, for each purchase we collect:

- **The mobile number(s) being topped up** (the MSISDN you enter as the recipient of an

airtime or data top-up).

- **Biller account references** (for example, the utility or biller account number you enter for a bill payment).
- **E-wallet payment metadata** received from your chosen e-wallet or payment gateway: the wallet used (Touch 'n Go eWallet, GrabPay or ShopeePay), masked or tokenised payment identifiers, transaction references, amounts and timestamps. We do not store your full e-wallet credentials or full card numbers.
- **Transaction records**: the products you bought, the recipient details above (in masked form where shown to you), the price, the payment channel and reference, and the order/transaction reference and date and time.

3.3 Registered distributors and dealers (business resellers with an account)

If you are a vetted business reseller with a Biller account, then in addition to the data in Section 3.1 we collect, through the App:

- **Account credentials and referral data**: the email address and password you set when you register, and the referral code you use to onboard.
- **Points-funding data (distributors)**: when a distributor tops up its closed-loop points, the bank-transfer reference entered and the bank-transfer receipt image uploaded to evidence the transfer. Note that an uploaded receipt image may itself contain mobile numbers and amounts.
- **Account and points-ledger records**: your account profile, the record of points funded by bank transfer at 1:1 (RM1 = 1 point) (distributors) or allocated to you (dealers), and your transaction history of purchases and points allocations made using your account.

When you register as a dealer, we collect, through the App, the **KYC document images** you upload for verification, namely your SSM business-registration document and your identity card (IC). Distributors are onboarded by us directly and provide their identity document and signed agreement during that onboarding. We collect KYC as document images only; we do not perform facial recognition, liveness checks or biometric matching on them (see Section 3.4).

Your closed-loop points are a prepaid right to buy in-app products from us. They are a

closed-loop, single-purpose, non-cashable usage right; their precise characterisation under the Financial Services Act 2013 and related instruments is addressed in the Distributor / Dealer Agreement. Points may be transferred only as a ledger entry between accounts within our closed distributor group (for example, from a distributor to that distributor's own downline dealer) and cannot be transferred to any party outside that group; any commercial settlement between a distributor and a dealer in respect of such a transfer takes place between those parties offline and outside the App, and we do not provide any cash-out, withdrawal or redemption of points for money.

3.4 Sensitive personal data and biometrics

Biller does **not** collect biometric data and does **not** use facial recognition, liveness checks or fingerprint matching for onboarding or any other flow.

One category of sensitive personal data can be present in what we collect: the IC/MyKad image uploaded for reseller KYC (Section 3.3) may, on its face, reveal the holder's religion (the MyKad of a Muslim holder displays the religion field). We do not use that information for any purpose; it is captured only because it appears on the document itself, and the image is protected with the security measures in Section 15. We rely on your explicit consent under section 40 of the PDPA for this processing, which we ask for as a separate, un-pre-ticked step when you upload your KYC documents. If we ever introduce any other processing of biometric or sensitive personal data, we will first update this Policy, identify it clearly, and obtain your explicit consent as the PDPA requires.

4. Why we process your personal data (purposes)

We process your personal data for the following purposes, each of which is directly related to operating Biller, is necessary for that purpose, and is adequate but not excessive:

- To complete your prepaid top-ups and bill payments by passing the necessary details to the relevant telco or biller.
- To process and reconcile your e-wallet payments and (for distributors) your points funding.
- To prevent, detect and investigate fraud, abuse and spam, including device attestation and integrity checks.

- To issue receipts and to provide you with your transaction history and order confirmations.
- To provide customer support and to handle disputes and our failed, incorrect or undelivered-transaction resolution (re-delivery or refund within our 24-hour resolution target, in addition to your statutory rights, see Section 14).
- To send you transaction and service notifications, where you have allowed them.
- To meet our legal, tax and regulatory record-keeping and reporting obligations.
- For registered distributors and dealers, to administer the closed-loop points facility and your account.

5. Our legal basis and your consent

We process ordinary personal data where processing is necessary for the performance of a contract with you, including completing the purchase you ask us to make, and otherwise on the basis of your consent. For a guest purchase, when you confirm your order and pay, we process the recipient and payment details you have entered so that we can carry out that transaction; this processing is necessary for the performance of that one-off contract with you. For registered distributors and dealers, we process your account, points and transaction data to perform our agreement with you and to operate your account.

You may decline to provide personal data, but some data is obligatory to provide the service (see Section 9). Where we rely on your consent, you may withdraw it (see Section 11), although withdrawal will not affect processing already carried out and may mean we can no longer provide the relevant service.

6. Source of your personal data

We obtain your personal data from the following sources:

- Directly from you, when you enter recipient numbers or biller references, make a purchase, or register and submit account or points-funding information.
- Generated by your device and the App's software, such as the app-generated installation identifier and the integrity/attestation and anti-fraud signals described above.
- From the e-wallet provider or payment gateway, through the payment confirmation or callback for your transaction.

7. Classes of third parties to whom we may disclose your personal data

We disclose your personal data only for the purposes in Section 4, or a directly related purpose, and only to the following classes of third parties:

- **Telcos, airtime aggregators and billers** (including Celcom / CelcomDigi, Digi, Maxis / Hotlink, U Mobile, redONE, onexox, and utility and other billers) to fulfil your purchase.
- **E-wallet providers and payment gateways** (including Touch 'n Go eWallet, GrabPay, ShopeePay and our acquiring payment gateway) to process and reconcile payments.
- **Fraud-prevention, attestation and messaging service providers** who act as our data processors, including **Google LLC** for the Google Play Integrity service and **Google Firebase Cloud Messaging** push-notification delivery (Android and iOS), and **Apple Inc.** for the Apple App Attest service.
- **Cloud hosting and IT service providers** who host and support the App and our systems.
- **Within the reseller network (dealers only)**: if you are a dealer, your business identity, your assigned rate profile and the points allocated to you are visible to the distributor to which your account is bound, so that the distributor can perform its role in the network.
- **Professional advisers, auditors and insurers** where reasonably necessary.
- **Government bodies, regulators and law enforcement agencies**, where we are required or permitted by law to disclose, or to protect our rights.

We do not sell your personal data. We do not disclose your personal data to any party outside the classes above without your consent, except where the PDPA permits or requires it.

Where we engage data processors, we bind them by written agreement to protect your personal data, to process it only on our instructions, and to comply with the Security Principle. Data processors are themselves directly responsible for the security of personal data under the PDPA.

8. Choices and how to limit processing

You can limit how we process your personal data by:

- Declining to provide data that is voluntary.

- Turning off push notifications in your device settings, or opting out of any non-essential messaging.
- Withdrawing your consent as described in Section 11.

If you enter the personal data of another person (for example, you top up a mobile number that belongs to someone else, or upload a receipt that contains another person's details), you confirm that you are entitled to provide that data and to have us process it for the purpose of the transaction, and that the other person is aware of this Policy.

9. Whether providing data is obligatory

Some personal data is obligatory: without it we cannot provide the service. In particular:

- The recipient mobile number or biller account reference and the payment data are obligatory to complete a purchase.
- Certain device, attestation and anti-fraud signals are required for us to accept and screen a transaction.
- For registered resellers, the email address and password are obligatory to operate an account; a referral code is obligatory for a dealer to register; the KYC document images (SSM and IC) are obligatory for a dealer to place any order; and the bank-transfer reference and receipt image are obligatory for a distributor to fund points.

If you do not provide obligatory data, the relevant purchase or account cannot proceed. Other data is voluntary and you may choose not to provide it.

10. How long we keep your personal data (retention)

We keep your personal data only for as long as necessary for the purposes in Section 4, after which we take reasonable steps to destroy or permanently delete it. In practice:

- Transaction and financial records are retained for the period required by Malaysian accounting, tax and other record-keeping law, and for the resolution of any dispute.
- Recipient mobile numbers, biller references and uploaded receipt images are minimised and are deleted or anonymised once they are no longer needed for the transaction, verification, fraud-prevention and the resolution window.
- Reseller KYC document images (SSM and IC) are retained, in secure storage, for the duration of the reseller account and for a further period after account closure as required

or permitted by applicable tax, record-keeping and fraud-prevention law, after which they are securely destroyed or permanently de-identified.
- Distributor and dealer account and points records are retained for the period required under applicable law and are then deleted.

If you ask us to delete your account or data, we will do so except where we are required or permitted by law to retain certain records (for example, transaction records kept as required by law).

11. Your rights

Under the PDPA you have the following rights, which you can exercise by contacting our DPO (Section 2):

- **Access**: you may request access to the personal data we hold about you.
- **Correction**: you may request that we correct personal data that is inaccurate, incomplete, misleading or out of date.
- **Withdrawal of consent**: you may withdraw your consent to our processing of your personal data, in writing, after which we will cease the relevant processing (this may affect our ability to provide the service).
- **Data portability**: you may request that we transmit your personal data to another data controller by electronic means, where this is technically feasible and the data formats are compatible.

To help us locate your records and act on your request, please give us enough detail to identify the relevant data. If you used the App as a guest, you have no account with us, so please quote the order/transaction reference and the recipient and payment details of the transaction concerned; we may ask for further information to verify that the request genuinely relates to you. We will respond to your request within the time and in the manner required by law. We may need to verify your identity before acting on a request, and in limited cases the law allows us to decline or charge a prescribed fee.

If you hold a registered reseller account (as a distributor or a dealer), you can also delete your account using the in-app account-deletion option in your settings. This self-service deletion is available to registered reseller accounts (both distributors and dealers); guests have no account and should use the DPO channel above to request erasure of their transaction data. In

either case we will still retain the minimum records the law requires us to keep.

12. Cookies, SDKs and analytics

The App is a mobile application and does not use website browser cookies. It does use software development kits (SDKs) and services that process limited data on our behalf, namely:

- **Device integrity and attestation** (Google Play Integrity on Android, Apple App Attest on iOS) for fraud prevention.
- **Push-notification delivery** (Google Firebase Cloud Messaging on Android and iOS), which uses a device push token to send you transaction and service messages.

We do not use third-party analytics, advertising or crash-reporting SDKs in the App. These tools process the device and anti-fraud signals described in Section 3 and do not access your contacts or files beyond what is needed for the functions above.

13. Children

The App and its services are intended for adults and are not directed at children. Consistent with our Terms and Conditions, we do not knowingly provide the Products to, or knowingly collect personal data from, anyone under 18. If you believe a child has provided us with personal data, please contact our DPO and we will take appropriate steps to delete it.

14. Relationship to your consumer rights

Nothing in this Policy limits or excludes the rights and guarantees you have as a consumer under the Consumer Protection Act 1999, which apply regardless of anything stated here. Our service commitments, including any resolution target for failed, incorrect or undelivered transactions, are in addition to, and do not replace, those statutory rights.

15. Security of your personal data

We take practical steps to protect your personal data against loss, misuse, modification, and unauthorised or accidental access, disclosure, alteration or destruction, having regard to the nature of the data, the place where it is stored, the security of our equipment, the reliability of our personnel, and the secure transfer of data. These measures include encryption of data in

transit using up-to-date transport security with certificate pinning, encryption at rest of sensitive data such as mobile numbers, receipt images and account information, access controls, and the redaction of mobile numbers in our logs. We also require our data processors, by contract, to apply appropriate security measures.

No method of transmission or storage is completely secure, but we work to protect your personal data and to keep our safeguards under review.

16. Cross-border transfers

Some of the processors we use operate outside Malaysia, so some of your personal data, including the bulk of your account and transaction data, is transferred to and processed outside Malaysia. The principal offshore locations are set out below:

- **Google LLC (Google Play Integrity and Firebase Cloud Messaging)** processes your device push token, the app-generated installation identifier and related message metadata on Google infrastructure, including in the **United States**.
- **Apple Inc. (App Attest)** processes attestation data, including in the **United States**.
- **Amazon Web Services (AWS)** hosts our application database (which holds account, recipient, transaction and points-ledger records) in the **ap-southeast-1 (Singapore)** region.
- **Cloudflare, Inc.** provides object storage (Cloudflare R2) for uploaded images, including receipt and KYC document images, on its global infrastructure.
- **Our payment gateway (DOKU)** processes payment-confirmation and reconciliation data for your e-wallet payments, including in **Indonesia**.

For each such transfer we rely on a basis permitted under section 129 of the PDPA, which may include that the destination ensures a level of protection substantially similar to, or at least equivalent to, the PDPA, that the transfer is necessary for the performance of our contract with you, your consent, or that we have taken all reasonable precautions and exercised all due diligence to ensure your data is protected. We keep a record of the offshore processors we use, their location, the data categories transferred, and the section 129 basis relied on for each, in line with the Commissioner's Cross-Border Personal Data Transfer guidance.

17. Data breach handling

We maintain an incident-response process for personal data breaches. If we have reason to believe a personal data breach has occurred, we will notify the Personal Data Protection Commissioner as soon as practicable, in the manner and form the Commissioner requires (under the Commissioner's current guidelines, within 72 hours). Where a breach causes or is likely to cause significant harm to affected individuals, we will also notify those individuals without unnecessary delay (under those guidelines, within seven days of notifying the Commissioner). We assess and document every breach, and we follow the timeframes and thresholds set out in the Commissioner's current guidelines.

18. Alignment with app store privacy disclosures

We are required by Google Play and the Apple App Store to provide accurate privacy disclosures. The data practices we declare in the **Google Play Data Safety** section and in the **Apple App Privacy** details are consistent with this Policy, including the categories of data we collect (such as phone number, email address (resellers), payment and financial information, user-uploaded images (bank-transfer receipts and KYC documents, resellers), and device or other identifiers), the purposes (app functionality and fraud prevention), the sharing of the push token and device/attestation signals with Google and Apple as described in Sections 7, 12 and 16, the use of encryption in transit, and the availability of a data-deletion path. We do not use your data to track you across other companies' apps or websites, and the app-generated installation identifier is not used for tracking.

19. How to contact us and how to complain

For any question, request or complaint about your personal data, please contact our DPO (Section 2) or our support team:

- Support email: support@biller.my
- Support telephone: +60172208661

20. Changes to this Policy

We may update this Policy from time to time to reflect changes in our practices or in the law. We will post the updated Policy in the App and at our published Privacy Policy URL, and we will change the "Last updated" date above. Where the law requires, we will tell you about material

changes and, where relevant, ask for your consent before collecting or using your personal data for a new purpose.

This Policy is governed by the laws of Malaysia.