Privacy Policy of Butler Pay

Last updated: October 23, 2026

This Privacy Policy (“Policy”) governs the collection, use, storage, disclosure, and protection of personal data of individuals processed while using Butler Pay, operated by Butler Finances Group Limited (hereinafter — “Company”, “we”, “us”, “Service”, “Solution”).
It applies to every surface on which we offer the Solution: the website butlerpay.app, the Butler Pay application for iOS, the Butler Pay application for Android, the Butler Pay Telegram Mini App, our Telegram bots, and the interfaces and APIs that support them (each, and together, the “Solution”). Where a rule applies to only one of those surfaces, this Policy says so.
Butler Finances Group Limited is the data controller for the personal data described here. We are the legal entity that provides the Service, and we are responsible for what is set out below.

1. General Provisions

1.1. This Policy applies to all Users, regardless of their location, when using the Solution, including the website, the mobile applications, the Telegram Mini App, APIs, referral programs, and other platforms administered by the Company.
1.2. By creating an account or otherwise using the Solution, you confirm that you have read and understood this Policy and that you agree to the processing of your personal data as described in it. Where we rely on your consent, we ask for that consent separately and you may withdraw it at any time under Section 15.
1.3. If you do not agree with the terms of this Policy, you must stop using the Solution. You may delete your account at any time under Section 14.
1.4. Butler Pay is a financial service. Some of the data described here is collected because law obliges us to collect it — in particular identity-verification (KYC) and anti-money-laundering (AML) data. Where that is the case, this Policy says so, and providing that data is a condition of holding an account rather than a choice.

2. Contact Information

Data controller: Butler Finances Group Limited
Registered office: Rm 10, 13A/F South Tower World Finance Ctr Harbour City 17 Canton Rd TST Hong Kong
Website: https://butlerpay.app
Email for all privacy matters: info@butlerpay.app
You may send inquiries, requests, complaints, consent withdrawals, and data-deletion requests regarding the processing of personal data to the email address above. You can also reach us from inside the app at any time through Profile ⍰ Help, which opens a support conversation with our team. We answer privacy requests within 30 calendar days.

3. Age Requirement

3.1. The Solution is intended for adults. You must be at least 18 years old to create an account or use the Service.
3.2. We do not knowingly collect personal data from children. The Solution is not directed to children, contains no content designed for children, and uses no third-party advertising or third-party analytics of any kind.
3.3. If we learn that we have collected personal data from a person under 18, we delete that data and close the account, except for records we are required by anti-money-laundering law to retain. If you believe a minor has provided us with personal data, contact us at info@butlerpay.app and we will act on it.

4. Data We Collect, and How We Collect It

We collect only what the Service needs in order to work, to keep your money safe, and to satisfy the financial regulations that apply to us. This section lists every category we collect and states how each one reaches us.

4.1. Data you give us directly, by typing it into the Solution or uploading it

- Account identifiers: email address and/or phone number, and — if you sign in with Apple, Google, or Telegram — the account identifier and the basic profile fields that provider returns to us. We collect these when you sign in or register. If you use Sign in with Apple and choose to hide your email address, we receive Apple's private relay address and never your real one.
- Profile data: your first and last name, and your display name, collected when you enter them.
- Identity-verification (KYC) data: full name, date of birth, gender, nationality, country, city, address line and post code, identity-document type and number, and Tax Identification Number where applicable. We collect these when you complete identity verification in order to obtain a card. This is a legal obligation, not an optional feature.
- Identity-document images: photographs of your identity document, which you upload from your device's photo library. We collect them only during identity verification.
- Financial and transactional data you enter: transfer amounts and recipients, SBP payment details, card top-up amounts, and eSIM plan selections, collected at the moment you make each request.
- Support content: the messages, attachments, and screenshots you send us through the in-app support conversation or through our Telegram support bot, collected when you send them.
- Approximate device location: the mobile app may ask for foreground location permission only when you tap «Я здесь» (I'm here) in delivery. Coordinates rounded to two decimal places (about 1 km) are sent once to suggest the nearest city and are never stored or logged. There is no background location access. The Telegram Mini App uses Telegram's location prompt in the same way.
- Referral data: a referral code you enter or an invitation link you open, collected when you use it.
- Preferences: your chosen language, appearance theme, and notification choices, collected when you set them.

4.2. Data generated automatically when you use the Solution

- Account identifier: an internal user identifier that we create for you and that accompanies every authenticated request you make. It exists so we can tell your data apart from another person's.
- Session and security data: session records, sign-in and sign-out times, the device type and operating-system version reported by your device, the IP address your requests arrive from, and the approximate country derived from that IP address for fraud-prevention purposes. We collect these automatically on each request. Device location is requested separately only when you tap «Я здесь» (I'm here) in delivery, as described in Section 4.1.
- Push notification identifiers: a push notification token issued to your device by Apple or Google, and a random installation identifier that our app generates for your installation of the app. We collect these only after you sign in and only if you allow notifications. See Section 9.
- Transaction and product records: card authorisations and declines reported to us by the card issuer, balance top-ups, ledger balances and entries, eSIM orders and profiles, and referral rewards. We record these as they happen.
- Technical logs: server-side records of requests to our systems, kept to detect abuse, diagnose faults, and satisfy audit requirements. These contain the identifiers above, not the content of your messages.
- Website usage data: on butlerpay.app only, basic technical information about the browser session, as described in Section 10.

4.3. Data we receive from third parties

- From our card-issuing partners: card status, the card's masked identifiers, authorisation and decline events, merchant names and amounts, and fees. We receive these through their APIs and callbacks.
- From payment processing partners: settlement status, deposit confirmations, and payout status for the transactions you initiate.
- From identity-verification and sanctions-screening sources used by us or by our card-issuing partner, including public records, government registries, and sanctions and politically-exposed-person lists, in order to meet anti-money-laundering obligations.
- From sign-in providers (Apple, Google, Telegram): the identifier and basic profile fields described in

Section 4.1, received when you choose to sign in with them.
- From a person authorised to act on your behalf, where you have appointed one.

4.4. Data we deliberately do NOT collect

The following are named explicitly so that this Policy can be checked against the privacy label published for our apps on the App Store and Google Play. We do not collect any of them:

- Background device location. We use approximate coordinates only on your request to suggest the nearest city in delivery, as described in Section 4.1. Any country inferred automatically for fraud prevention is derived from the IP address of a request.
- Your contacts or address book.
- Health, fitness, or medical data.
- Biometric data. The apps do not use Face ID, Touch ID, fingerprint unlock, or any face-matching, and we never receive biometric information from your device.
- Microphone audio or video recordings. The microphone permission is explicitly disabled in our apps.
- Advertising identifiers, including Apple's Identifier for Advertisers (IDFA) and the Google Advertising ID.
- Your browsing or search history outside our own Solution, and the list of other apps installed on your device.
- Crash and performance telemetry from your device. Our apps bundle no crash-reporting, analytics, attribution, or advertising SDK.

5. Device Permissions and Data Stored on Your Device

5.1. Our mobile apps request only the permissions below. Each is requested at the moment the related feature is used, never at launch, and each can be refused or withdrawn in your device settings. Refusing a permission disables only the feature that needs it; the rest of the app continues to work.

- Camera — used solely to scan payment QR codes. We do not record video, we do not take photographs with it, and no image from the camera leaves your device except the decoded content of a QR code you deliberately scan.
- Photo library — used solely so that you can choose a photograph of your identity document to upload for account verification. We access only the item you pick.
- Foreground location — requested only when you tap «Я здесь» (I'm here) in delivery, to suggest the nearest city from approximate coordinates. We do not request background location permission. The Telegram Mini App uses Telegram's location prompt for the same purpose.
- Notifications — used to deliver the transaction, security, and support alerts described in Section 9. This permission is requested only after you have signed in.

5.2. Some data stays on your device and is never sent to us: your session token, your language and appearance preferences, the flag recording that you have seen the introduction, and the random installation identifier used for notifications. These are held in the operating system's protected storage (Keychain on iOS, Keystore-backed storage on Android) and are erased when you delete the app.
5.3. Our apps transmit data to our servers only over encrypted HTTPS connections. Insecure connections are blocked at the operating-system level by our app configuration.

6. How We Use Your Data

This is the complete list of what we use your personal data for. We use it for nothing else, and we do not repurpose data collected for one of these purposes for a different one without asking you first.

- To create and operate your account, authenticate you, keep you signed in, and let you manage and revoke your own sessions.
- To verify your identity (KYC) and to carry out the anti-money-laundering, sanctions-screening and risk checks that financial regulation requires of us.

- To provide the Service you ask for: issuing, funding, freezing and closing cards; holding balances; executing transfers, top-ups and withdrawals, SBP payments and currency conversion; and purchasing and managing eSIM plans.
- To display your own data back to you — balances, transaction history, card details, orders and statements.
- To operate the referral programme, attribute invitations, and calculate and pay rewards.
- To provide customer support, and to answer your questions and complaints.
- To send you service and security messages — one-time sign-in codes, transaction confirmations, security alerts, and notices about changes to the Service or to this Policy. These are not marketing, and we send them for as long as you hold an account.
- To detect, investigate and prevent fraud, unauthorised access, abuse of the Service, and financial crime, and to protect the security and integrity of the Solution.
- To keep the accounting, tax, audit and regulatory records that law requires us to keep.
- To establish, exercise or defend legal claims, and to respond to lawful requests from competent authorities.
- To maintain and repair the Service — diagnosing faults from our own server-side logs, not from telemetry taken off your device.

6.1. Marketing. We send marketing email only to people who have separately and voluntarily subscribed to our newsletter on the butlerpay.app website. Our mobile apps do not enrol you in marketing, having an account does not enrol you in marketing, and we do not build marketing profiles from your account, transaction or usage data. Every marketing email carries an unsubscribe link, and you can also unsubscribe by writing to info@butlerpay.app.
6.2. We do not sell your personal data. We have never sold it, and we do not share it with data brokers or advertising networks.

7. Legal Basis for Processing

We rely on the following legal bases:

- Performance of a contract with you — to operate your account and execute the transactions you request.
- Compliance with a legal obligation — for identity verification, anti-money-laundering and sanctions checks, record-keeping, tax and accounting, and responses to lawful authority requests.
- Our legitimate interests — to prevent fraud and abuse, to secure the Solution, and to defend legal claims. We balance these against your rights and do not rely on this basis where your interests override ours.
- Your consent — for device notifications, for optional uploads, and for the newsletter. Where consent is the basis, you may withdraw it at any time under Section 15, with no effect on the lawfulness of processing carried out before withdrawal.

8. No Tracking, No Advertising, No Third-Party Analytics

8.1. We do not track you. We do not link the data collected through our apps with data from third parties for advertising or advertising measurement, and we do not share it with data brokers.
8.2. Our iOS app does not use the App Tracking Transparency framework and will never ask for permission to track you across other companies' apps and websites, because it performs no such tracking. It does not collect Apple's Identifier for Advertisers (IDFA), and our Android app does not collect the Google Advertising ID.
8.3. Our mobile apps contain no advertising SDK, no attribution SDK, no third-party analytics SDK, and no third-party crash-reporting SDK. No advertising is displayed in the Solution.
8.4. Every category of data described in Section 4 is collected for app functionality, security, support, and legal compliance only, and is linked to your account because it is written against your authenticated session. This matches the privacy information we publish for our apps on the App Store and Google Play.

9. Push Notifications

9.1. If you allow notifications, your device is issued a push token by Apple Push Notification service (on iOS) or Firebase Cloud Messaging (on Android). We store that token together with a random identifier our app generates for your installation, your account, and your language, so that we can address a message to the right device in the

right language.
9.2. The installation identifier is random, specific to your installation of our app, and is not a device fingerprint. It is not shared with anyone, it is not used to recognise you anywhere else, and it ceases to exist when you delete the app.
9.3. Notifications are used only to tell you that something has happened in your account — a deposit, a card transaction, a security event, a support reply. They are not used for marketing.
9.4. We delete the registration for your device when you sign out, and you can turn notifications off at any time in your device settings. Notifications are never a condition of using the Service or of receiving anything from us.

10. Cookies and Similar Technologies

10.1. This section applies to the butlerpay.app website only. Our mobile applications do not use cookies, tracking pixels, web beacons, or advertising identifiers.
10.2. On the website we use cookies and local storage to:

- Keep you signed in to your web session, in a cookie that the page scripts cannot read
- Remember your language and interface preferences
- Protect forms and sign-in against abuse

10.3. We do not use advertising cookies, we do not run third-party advertising or analytics tags, and we do not use cookies to build a profile of you or to personalise advertising.
10.4. Cookies may be session-based (deleted when you close the browser) or persistent (stored for a defined period). You can manage or delete cookies in your browser settings; disabling the strictly necessary ones will prevent you from signing in.

11. Sharing Your Data with Third Parties

11.1. We share personal data only where it is necessary for one of the purposes listed in Section 6, and only with the categories of recipient below. Each entry states what is shared and why.

- Card-issuing partner Valut (https://pro.valut.com) — the provider that issues and operates your cards. It receives your name, the identity-verification data and document images required by their own regulator, the cardholder contact address we generate for the card, and the transaction instructions you make. This sharing is necessary to issue a card and is disclosed to you before you apply for one.
- Payment processing partners — receive the payment details necessary to execute a bank or SBP payment you have initiated.
- eSIM supply partner — receives the order details needed to provision the mobile data plan you purchased. It does not receive your identity-verification data.
- Email delivery provider (Postmark, operated by ActiveCampaign) — receives your email address and the content of the transactional message so that one-time codes and service notices reach you.
- Push notification infrastructure (Expo Application Services, Apple Push Notification service, and Google Firebase Cloud Messaging) — receives the push token and the notification text needed to deliver a message to your device.
- Sign-in providers (Apple, Google, Telegram) — where you choose to sign in with them, they authenticate you and return the identifier described in Section 4.1. We send them no account or transaction data.
- Cloud hosting and object-storage providers — host our servers, databases and uploaded files under contract, and process data only on our instructions.
- Professional advisers — lawyers, auditors and accountants, bound by professional confidentiality, where needed for advice, audit or the defence of a claim.
- Competent authorities — regulators, tax authorities, law-enforcement and courts, where we are legally obliged to respond or where disclosure is necessary to establish, exercise or defend a legal claim.
- A successor entity — in a merger, acquisition or sale of assets, in which case the recipient is bound by this Policy and you are notified before your data becomes subject to a different one.

11.2. We do not sell personal data, we do not rent or trade it, and we do not disclose it to advertising networks,

data brokers, or third-party analytics providers.
11.3. A current list of the specific processors we use is available on request from info@butlerpay.app. We may replace a provider with an equivalent one, which is then bound by the same obligations described in Section 11.4.

11.4. Equal protection by every recipient

We confirm that every third party with whom we share your personal data — including service providers, third-party software development kits used in our applications, payment, card and eSIM partners, and any parent, subsidiary, affiliate or other related entity that has access to that data — is required by written agreement to provide the same or equal protection of your personal data as is stated in this Policy.
Those agreements bind each recipient to: process the data only on our documented instructions and only for the purpose for which it was shared; apply confidentiality obligations to their personnel; maintain technical and organisational security measures at least equivalent to ours; not sell the data, use it for their own advertising, or use it to build or enrich a profile of you; impose the same obligations on any sub-processor they engage, and remain responsible to us for that sub-processor; assist us in answering your rights requests and in notifying data breaches; and delete or return the data when the engagement ends, except where law requires them to retain it.
Where a recipient is itself a regulated financial institution acting as a controller of the data in its own right, it is additionally bound by the financial-services confidentiality and data-protection rules of its own regulator.

12. International Data Transfers

12.1. We operate internationally, and the recipients described in Section 11 may be located outside your country of residence, including in jurisdictions whose data-protection laws differ from your own.
12.2. Where personal data is transferred across borders, we put appropriate legal safeguards in place before the transfer — in particular standard contractual clauses or equivalent contractual protections, together with the obligations set out in Section 11.4 — so that your data continues to receive the protection described in this Policy.
12.3. You may request further information about the safeguards applied to a specific transfer by writing to info@butlerpay.app.

13. Data Retention

13.1. We keep personal data only as long as is necessary for the purpose it was collected for, or for the period law requires, whichever is longer. The periods we apply are:

- Account and profile data — for as long as your account is open, then deleted or anonymised once the periods below have elapsed.
- Identity-verification data and document images — at least five (5) years after the end of our business relationship with you, because anti-money-laundering law requires it. We cannot shorten this period at your request.
- Transaction, ledger and card records — at least five (5) years after the transaction, for anti-money-laundering, accounting and tax purposes; longer where a specific tax or audit rule requires it.
- Support conversations — up to three (3) years after the conversation ends, so that we can evidence how a complaint was handled.
- Session records and technical security logs — up to twelve (12) months, then deleted.
- Push notification registrations — until you sign out, revoke the notification permission, or delete the app.
- Newsletter subscription data — until you unsubscribe, plus a minimal suppression record so that we do not email you again.
- Data connected with a legal claim, investigation or regulatory request — until that matter is finally resolved, after which the periods above resume.

13.2. When a retention period expires, the data is deleted or irreversibly anonymised. Anonymised data no longer identifies you and is not subject to this Policy.
13.3. Backups are retained on a rolling schedule and are overwritten in the ordinary course. Data deleted from our live systems is removed from backups as those backups expire, and is not restored to live systems in the meantime.

14. Deleting Your Account and Your Data

14.1. You can start account deletion from inside the app at any time: open Profile, tap “Delete account”, and confirm. That opens a support conversation with our team, which is the step regulation obliges us to add — Butler Pay holds money and may have cards open in your name, so an account cannot be erased by a single tap without first settling those balances and closing those cards. We confirm the request, tell you what has to be settled, and then carry the deletion out.
14.2. You can equally request deletion by writing to info@butlerpay.app from the address registered on your account.
14.3. What happens then: we close your cards, return any remaining balance to you, terminate your sessions, and delete your profile, preferences, support content, device registrations, uploaded files and referral data. Your account can no longer be signed in to.
14.4. What we must keep, and why: identity-verification records and transaction records are retained for the periods set out in Section 13.1 because anti-money-laundering, accounting and tax law require us to retain them. This retained set is locked down — it is used only to satisfy those legal obligations and to answer a lawful request from an authority, and it is never used to contact you, to profile you, or for any other purpose. It is deleted when its retention period ends. No other applicable law permits us to shorten it, and this limitation is disclosed to you here so that the scope of deletion is clear before you ask for it.
14.5. Deleting the app from your device is not the same as deleting your account. Removing the app erases the data stored on your device (Section 5.2) but leaves your account open on our systems. Use the in-app flow in Section 14.1 to close the account itself.

15. Withdrawing Your Consent

15.1. Where we process data on the basis of your consent, you can withdraw that consent at any time, and withdrawing it is always as easy as giving it:

- Notifications — turn them off in your device settings, or sign out; we then stop sending them and delete the device registration.
- Camera and photo-library access — revoke the permission in your device settings at any time.
- Newsletter — use the unsubscribe link in any marketing email, or write to info@butlerpay.app.
- Any other consent-based processing — write to info@butlerpay.app and tell us what you are withdrawing.

15.2. Withdrawal takes effect as soon as we act on it and does not affect the lawfulness of processing carried out before it. Withdrawing consent does not remove our obligation to keep the records described in Section 13.1, because those are kept under a legal obligation rather than under your consent.
15.3. You will never be charged, penalised, or given a degraded version of the Service for withdrawing a consent, except that a feature which genuinely depends on the permission you withdrew will stop working.

16. Your Privacy Rights

16.1. Subject to the law that applies to you, you have the right to:

- Be told what personal data we hold about you and why, and obtain a copy of it
- Have inaccurate or incomplete data corrected or updated
- Have your data deleted (the “right to be forgotten”), within the limits set out in Section 14.4
- Restrict or object to processing carried out on the basis of our legitimate interests
- Receive the data you provided to us in a structured, commonly used, machine-readable format, and have it transmitted to another controller where technically feasible
- Withdraw consent, as described in Section 15
- Opt out of marketing communications at any time
- Not be subject to a decision based solely on automated processing that produces legal effects concerning you, as described in Section 17
- Lodge a complaint with your national data protection authority

16.2. To exercise any of these rights, write to info@butlerpay.app from the address registered on your account, or open a support conversation in the app. We answer within 30 calendar days. If a request is exceptionally complex we may extend that period and will tell you why before the first 30 days are up.
16.3. We may ask you to verify your identity before acting on a request. This is a protective measure — it stops someone else obtaining or deleting your data — and we ask only for what is needed to confirm that the request is yours.
16.4. Exercising a right is free. We charge nothing for a first copy of your data, and we do not restrict your access to the Service because you exercised a right.

17. Automated Processing and Profiling

17.1. We use automated processing in a limited and specific set of cases, all of them concerned with safety and eligibility rather than with marketing:

- Fraud and abuse detection — for example, flagging an unusual transaction pattern, or automatically freezing a card after repeated declined authorisations
- Anti-money-laundering and sanctions screening, including checks performed by our card-issuing partner
- Automated checks on whether you meet the eligibility conditions for a card, a transaction limit, or a referral reward

17.2. We do not use automated processing or profiling for advertising, for marketing, for content personalisation, or to infer characteristics about you beyond what the checks above require.
17.3. In relation to automated processing, you have the right to:

- Request information about the logic involved, and the significance and likely consequences of the processing for you
- Request human intervention and a review by a member of our staff
- Express your point of view and contest the outcome
- Appeal a decision by writing to info@butlerpay.app or through in-app support

17.4. Where an automated check blocks a transaction or restricts an account, a person reviews the case on request. Some outcomes required by anti-money-laundering law cannot be reversed on appeal, and where that is so we tell you.

18. How We Protect Your Data

18.1. The Company implements technical, organisational and legal measures to protect personal data against unauthorised access, alteration, destruction, disclosure, accidental loss, and unlawful processing.
18.2. Those measures include:

- Encryption of all data in transit over TLS; insecure connections are refused by our applications
- Encryption at rest of particularly sensitive values, including two-factor authentication secrets and stored identity-document numbers
- Segmented access, least-privilege authorisation, and separation of our internal staff systems from the public Service
- Database-backed sessions that can be revoked instantly, and that you can revoke yourself from the app
- Optional two-factor authentication on your account, which we recommend you enable
- Append-only audit trails for staff actions on customer data, and security logging and monitoring
- Protection against denial-of-service and malicious traffic, and regular testing of our infrastructure
- Private delivery of uploaded documents: your identity-document images are not publicly addressable and are served only to an authenticated, authorised request

18.3. Our staff are trained on personal data processing and protection, are bound by confidentiality, and may access customer data only where their role requires it and where that access is recorded.
18.4. No system is perfectly secure. If a personal data breach occurs that is likely to result in a risk to your rights,

we notify the competent supervisory authority and, where the risk to you is high, we notify you directly and without undue delay, describing what happened, what data was involved, and what you can do.

19. External Links and Third-Party Services

19.1. The Solution may contain links to third-party websites and services, and may open a third party's screen — for example a sign-in provider — inside your browser. The Company does not control their privacy policies or security practices, and this Policy does not apply to them. We recommend reviewing their policies separately.

20. Changes to This Policy

20.1. We may amend this Policy. The date at the top of this document always shows when it was last changed, and the current version is published at butlerpay.app/privacy-policy and linked from inside the apps.
20.2. For a material change — one that alters what we collect, what we use it for, or who we share it with — we notify you in advance by email or through an in-app notice, and where the change requires your consent we ask for it before the change applies to you.
20.3. Continued use of the Solution after a change takes effect indicates acceptance of the revised Policy. If you do not accept it, you may delete your account under Section 14.

21. Governing Law and Jurisdiction

21.1. This Policy is governed by and construed in accordance with the laws of the Hong Kong Special Administrative Region, the Company's jurisdiction of incorporation, without prejudice to any mandatory data-protection rights you hold under the law of your own country of residence.
21.2. Disputes regarding the processing of personal data shall be resolved by the competent courts of that jurisdiction. This does not prevent you from lodging a complaint with the data protection authority of your country of residence.