HYLPERS US - PRIVACY POLICY

Effective Date	Effective upon US launch
Version	Full US Privacy Policy - Stripe/Checkr - 2026.06.27
Company	Hylpers Inc., California, U.S.A.
Region	United States
Payment Provider	Stripe or approved third-party provider
Background Check Provider	Checkr or approved third-party provider, where applicable
Support Email	support@hylpers.com

1. Important Notice

This US Privacy Policy explains how Hylpers Inc. and approved Hylpers affiliates collect, use, disclose, store, and protect personal information when users access or use the Hylpers website, mobile application, customer support channels, provider onboarding flows, payment environment, booking tools, communications, background check workflows where applicable, optional promotional features, and related services in the United States.

Hylpers is a marketplace platform that connects Service Seekers with independent Service Providers. Hylpers does not employ Providers, does not directly perform the services listed by Providers, and does not act as a staffing agency, recruitment agency, or direct service provider unless expressly stated in writing.

2. Scope and Launch Status

- Service Seekers, Service Providers, company account users, website visitors, app users, customer support contacts, and prospective users in the United States.
- Hylpers websites, the Hylpers mobile application, social media lead forms, onboarding campaigns, Stripe payment/KYC flows, Checkr background check flows where applicable, optional provider promotional features, and support channels.
- Unless Hylpers confirms that US services are live, US legal pages should be marked “Effective upon US launch.”

3. Age Eligibility

Hylpers is intended only for users who are 18 years old or older. Hylpers does not knowingly allow persons below 18 years old to create accounts, provide services, request services, or submit payment, tax, or background check information. If Hylpers becomes aware that a person below 18 has submitted personal information, Hylpers may delete the account and related information, subject to legal, fraud-prevention, dispute, safety, or recordkeeping requirements.

4. Personal Information We Collect

Category	Examples	Purpose
Account information	Name, email address, mobile number, password credentials, account role, preferred language, country/state.	Account creation, login, communication, account support, fraud prevention.
Profile information	Profile photo, service categories, skills, service descriptions, work availability, experience, ratings, reviews, service areas.	Provider discovery, service listings, booking, quality control, trust and safety.

Stripe payment/KYC status information	Stripe account references, onboarding status, verification status, account capability status, payout status, transaction IDs, refund status, dispute/chargeback status, tax reporting status.	Payment authorization, capture, refunds, payouts, fraud prevention, compliance, support, dispute handling.
Checkr background check information	Background check status, eligibility status, report status, badge eligibility, adverse action status where applicable and legally permitted.	Provider safety review, category eligibility, badge approval, compliance, platform safety.
Location information	Approximate or precise location if permission is enabled, map location, service area, booking address, GPS or device-based location where allowed.	Nearby provider matching, booking support, safety, fraud prevention, service-area display.
Booking and transaction data	Service request, provider acceptance, booking date/time, amount, Hylpers convenience fee, taxes if applicable, cancellation, refund, dispute records.	Booking administration, payment processing, settlement, tax records, support, dispute review.
Communications and support data	Messages, emails, call notes, social media inquiries, complaint evidence, screenshots, support tickets.	Customer service, dispute resolution, safety investigation, quality review.
Device, app, and website data	IP address, device ID, operating system, app version, browser type, crash logs, analytics, cookies, session data.	Security, debugging, analytics, service improvement, fraud prevention.
Marketing and advertising data	Campaign source, consent preferences, ad interactions, referral codes, landing page visits, promotional feature performance.	Marketing, campaign measurement, remarketing where permitted, user communication preferences, marketplace analytics.

5. Information Hylpers Does Not Directly Collect Where Handled by Stripe or Checkr

Hylpers does not directly collect or store full card numbers, full bank account details, Social Security numbers, or full government identification documents in the Hylpers app database where such information is collected and processed directly by Stripe, Checkr, or another approved third-party provider.

Hylpers may store limited references, statuses, records, and compliance information required to operate the platform, process payments, manage payouts, review disputes, prevent fraud, conduct safety checks where applicable, and comply with legal obligations.

6. Stripe Payment and KYC Processing

Payments, payouts, identity verification, tax reporting, fraud prevention, sanctions screening, and payment compliance checks may be processed by Stripe or another approved third-party payment provider.

Stripe may collect and process information required to complete payment processing, payout processing, identity verification, tax reporting, account onboarding, fraud prevention, and compliance checks. This may include legal name, date of birth, address, tax identification information, bank account or debit card details, government identification information, and other information required by Stripe.

Hylpers may receive limited information from Stripe, including payment status, payout status, verification status, account status, transaction references, dispute status, tax reporting status, and other information reasonably required to operate the platform. Hylpers does not control Stripe internal processing systems.

7. Checkr Background Check Processing

For certain Service Provider categories, Hylpers may use Checkr or another approved background check provider to conduct background checks.

Checkr may collect and process information required to complete a background check, which may include personal identifiers, address history, date of birth, Social Security number, driver license information, consent forms, criminal history search results, motor vehicle records where applicable, or other information needed for the background check package selected.

Hylpers may receive background check status, report information, eligibility indicators, or other information from Checkr where legally permitted and reasonably required for platform safety, verification, category access, badge approval, or compliance review.

Where legally required, Hylpers will provide required notices, obtain consent, allow review, and follow applicable adverse action procedures before making a final negative decision based on a background check.

8. How We Collect Personal Information

- Directly from users when they create an account, complete a profile, list services, book services, contact support, or participate in promotions.
- Automatically through the website, mobile application, cookies, analytics tools, device permissions, payment environment, and security logs.
- From Stripe, Checkr, payment processors, background check providers, app stores, SMS/email providers, analytics providers, support tools, social media lead forms, advertising/marketing tools, and other approved third-party service providers.
- From other users when they submit ratings, reviews, complaints, booking feedback, dispute evidence, or safety reports.

9. How We Use Personal Information

- Create, manage, verify, secure, and support user accounts.
- Connect Service Seekers with independent Providers through search, maps, listings, availability, booking, and communications features.
- Process bookings, convenience fees, taxes where applicable, refunds, chargebacks, Provider payouts, optional promotional fees, reconciliation, and financial reporting.
- Support Stripe onboarding, payment/KYC verification, payout readiness, tax reporting, fraud prevention, and dispute review.
- Support Checkr background checks, category access, badge approval, safety review, and adverse action processes where applicable.
- Provide customer support, handle complaints, investigate disputes, enforce platform rules, suspend or remove accounts, and maintain trust and safety.
- Improve the app, website, service categories, pricing displays, user experience, security, analytics, and marketplace performance.
- Send OTPs, booking updates, account notices, legal updates, safety notices, background check notices where applicable, payment notices, promotional communications where permitted, and marketing communications subject to preferences.
- Comply with applicable federal, state, local, app store, tax, consumer protection, payment, background check, privacy, court, regulator, and law-enforcement requirements.

10. Sharing of Personal Information

Hylpers may share personal information only as reasonably necessary for platform operation, user safety, compliance, and service delivery. This may include sharing with:

- Other users, but only where needed for bookings, provider profiles, ratings, reviews, service-area visibility, and dispute handling.

- Stripe or other payment providers, acquiring banks, payout partners, fraud monitoring providers, tax reporting providers, and financial institutions.
- Checkr or other background check providers where applicable.
- SMS, email, OTP, hosting, cloud, analytics, app performance, customer support, legal, accounting, tax, security, and professional service providers.
- App stores and platform providers, including Apple and Google, where required for app distribution, privacy disclosures, crash reports, app analytics, and platform compliance.
- Government authorities, regulators, courts, law enforcement, or other parties where required by law, court order, lawful request, payment dispute, safety investigation, background check process, or legal obligation.
- Affiliates, successors, investors, or acquirers in connection with corporate restructuring, financing, merger, acquisition, asset sale, or due diligence, subject to confidentiality and legal safeguards.

Hylpers does not sell personal information in the ordinary meaning of selling user data for money. If applicable privacy laws define “sell” or “share” more broadly, Hylpers will comply with applicable disclosure and opt-out requirements.

11. Location Data

Hylpers may use location information to show nearby Providers, calculate service areas, help users find available services, improve safety, and support fraud prevention. Users may control device-level location permissions through device settings. If precise location is disabled, some app features may not work properly.

12. Cookies, Analytics, and Advertising

Hylpers websites may use cookies and similar technologies for essential functionality, security, analytics, performance measurement, campaign tracking, and marketing. Hylpers may use approved analytics and advertising tools to measure user acquisition, improve campaigns, evaluate optional promotional features, and improve marketplace performance. Where required, users may be offered cookie choices or browser/device controls.

13. Data Retention

Hylpers keeps personal information only for as long as reasonably necessary for the purposes described in this Privacy Policy, unless a longer retention period is required or permitted by law. Booking, payment, payout, refund, dispute, chargeback, fraud prevention, tax, accounting, background check, safety, and legal records may be retained for a longer period where necessary to protect Hylpers, users, Providers, and third parties.

14. Account Deletion and Data Deletion

Users may request deletion of their Hylpers US account through the app, through the Hylpers website, or by contacting support@hylpers.com. Recommended US web page: /us/delete-account.

When a valid deletion request is received, Hylpers will delete or anonymize personal information that is no longer required for legitimate business, legal, safety, tax, accounting, fraud prevention, payment, dispute, background check, or compliance purposes.

Some information may be retained where necessary for payment records, booking history, refunds, cancellations, disputes, chargeback prevention, fraud protection, Stripe transaction, payout or tax records, Checkr background check records or status history where legally permitted or required, tax/accounting/legal compliance, safety, security, abuse prevention, and enforcement of Hylpers Terms & Conditions.

Where Hylpers uses Stripe, Checkr, or other third-party providers to process payment, payout, KYC, or background check information, Hylpers may request deletion or restriction of relevant data from those providers where applicable and legally permitted.

15. US Privacy Rights

Depending on the user state of residence and applicable law, users may have the right to request that Hylpers confirm whether Hylpers processes their personal information, provide access, correct inaccurate information, delete personal information subject to exceptions, provide a copy of certain information, opt out of certain types of data sharing where applicable, limit certain uses of sensitive personal information where applicable, and appeal certain privacy request decisions where required by law.

Requests may be submitted through the app or by contacting support@hylpers.com. Hylpers may require reasonable verification before acting on a request to protect user privacy and account security.

16. Background Check Rights

Where background checks are used, Service Providers may have rights under applicable federal, state, and local laws. These may include the right to receive required disclosures, provide consent, receive certain notices, review applicable background check information, dispute inaccurate information with the background check provider, and receive required adverse action notices where applicable.

Service Providers may contact support@hylpers.com for Hylpers support matters and may also be directed to Checkr for background check report or dispute processes where applicable.

17. Security

Hylpers uses reasonable technical, organizational, and administrative measures designed to protect personal information. However, no website, app, payment process, background check process, or storage system is completely secure. Users are responsible for protecting their account credentials, OTPs, and devices.

18. International Transfers

Hylpers may process and store personal information in the United States, United Arab Emirates, and other countries where Hylpers, its affiliates, or approved service providers operate. Where applicable, Hylpers will use reasonable contractual, technical, and organizational safeguards for cross-border transfers.

19. Marketing Communications

Hylpers may send service-related messages and, where permitted, marketing or promotional communications. Users may opt out of marketing communications where required by law, but may still receive important account, booking, payment, background check, legal, safety, or support messages.

20. Changes to this Privacy Policy

Hylpers may update this Privacy Policy from time to time. Material updates may be notified through the app, website, email, or other reasonable method. Continued use of Hylpers after an update means the user acknowledges the updated Privacy Policy, unless otherwise required by law.

21. Contact

For account deletion, privacy requests, refund requests, cancellation concerns, disputes, chargeback questions, background check support, or general support matters, users may contact support@hylpers.com. Users should include their registered name, registered mobile number or email address, booking reference if applicable, and a clear explanation of the request.