FlexiWork Privacy Policy

Last Updated: 11 January 2026
Version: 1.0
Effective Date: 11 January 2026

FlexiWork Pte. Ltd. (UEN: 202550322H), with registered address at 60 Paya Lebar Road, #06-28, Paya Lebar Square, Singapore 409051 ("FlexiWork", "we", "our", "us") is committed to protecting your privacy and Personal Data.

This Privacy Policy explains:

- What Personal Data we collect
- How we use, disclose, and protect your Personal Data
- Your rights regarding your Personal Data
- How we comply with Singapore's Personal Data Protection Act 2012 (PDPA), Platform Workers Act 2024, EU General Data Protection Regulation (GDPR), and UK Data Protection Act 2018 & UK GDPR

BY USING THE FLEXIWORK PLATFORM, YOU CONSENT TO THE COLLECTION, USE, AND DISCLOSURE OF YOUR PERSONAL DATA AS DESCRIBED IN THIS PRIVACY POLICY.

---

1. SCOPE AND APPLICABILITY

1.1 Geographic Scope

FlexiWork Pte. Ltd. is incorporated in Singapore and operates as follows:

Primary Operations:

- Singapore-based company subject to Singapore laws and regulations
- Marketplace Services (shift-based work connections) currently available in **Singapore only**

SaaS Platform Services:

- Scheduling, time tracking, training, communication tools available **globally**
- Users worldwide can access SaaS features
- Users outside Singapore cannot access Marketplace Services (posting/applying for shifts) until expansion to their jurisdiction

Applicable Regulations:

- **Singapore:** Personal Data Protection Act 2012 (PDPA), Platform Workers Act 2024
- **European Union:** General Data Protection Regulation (GDPR)
- **United Kingdom:** UK Data Protection Act 2018, UK GDPR
- We comply with the strictest applicable standard for each user based on location

1.2 Data Controller

FlexiWork Pte. Ltd. (UEN: 202550322H) is the Data Controller for all users globally.

- **Singapore address:** 60 Paya Lebar Road, #06-28, Paya Lebar Square, Singapore 409051
- **For EU/UK users:** FlexiWork acts as Data Controller under GDPR/UK GDPR
- **EU Representative:** [To be appointed if required under GDPR Art. 27 - details will be provided]

---

2. DEFINITIONS

"Personal Data" means any information relating to an identified or identifiable individual, including:

- Name, NRIC/passport number, date of birth
- Contact information (email, phone, address)
- Financial information (bank account, payment details)
- Employment and work history
- Location data (GPS coordinates)
- Online identifiers (IP address, device ID, cookies)
- Biometric data (facial recognition for identity verification)
- Any other information that can identify you directly or indirectly

"Processing" means any operation performed on Personal Data, including collection, recording, storage, use, disclosure, transmission, erasure, or destruction.

"Data Subject" means you, the individual to whom Personal Data relates.

"Sensitive Personal Data" / **"Special Categories of Personal Data"** means:

- Health data
- Biometric data (when used for unique identification)
- Racial or ethnic origin (only as inferred from NRIC for verification—not used for profiling)
- We do NOT collect: Political opinions, religious beliefs, trade union membership, genetic data, data concerning sex life or sexual orientation

"Consent" means freely given, specific, informed, and unambiguous agreement to Processing of Personal Data.

---

3. DATA PROTECTION PRINCIPLES

We Process Personal Data in accordance with:

Singapore PDPA Principles:

- Consent, Purpose Limitation, Notification, Access & Correction, Accuracy, Protection, Retention Limitation, Transfer Limitation, Openness, Accountability

GDPR/UK GDPR Principles:

- Lawfulness, Fairness, Transparency, Purpose Limitation, Data Minimisation, Accuracy, Storage Limitation, Integrity & Confidentiality, Accountability

---

4. WHAT PERSONAL DATA WE COLLECT

4.1 Information You Provide Directly

During Registration (Workers):

- Full legal name, NRIC number
- Date of birth, gender, nationality
- Residential address, mobile phone, email
- Emergency contact (name, relationship, phone)
- Bank account details (for payment transfers)
- Profile photo (optional), work experience, skills, languages
- Availability and preferred work locations

During Registration (Employers):

- Individuals: Full name, NRIC/passport, contact details
- Companies: Company name, UEN, business registration documents, authorized representative details
- Bank account or payment method details

Identity Verification:

- NRIC (front and back), selfie with NRIC (facial verification)
- Passport (in limited cases)
- Business registration documents (for Employers)
- Proof of address

Platform Workers Act Compliance Data (Workers Only - Singapore):

- CPF account number (for MediSave contributions)
- Monthly earnings data (for contribution calculations)
- Work history on Platform (for compliance reporting)
- Work Injury Compensation (WIC) claims data (if applicable):
    - Injury reports and incident details
    - Medical certificates and treatment records
    - Hospital bills and receipts
    - Shift details at time of injury

During Platform Use:

- Shift postings, applications, availability confirmations
- Platform messages between Employers and Workers
- Reviews and ratings (1-5 stars, written reviews)
- Support inquiries (emails, chat transcripts)
- Dispute information (evidence, documentation)
- Training progress (modules completed, quiz scores, awareness-level certificates)

Payment and Financial Information:

- Bank account details for direct payment transfers (Workers) or refunds (Employers)
- Payment history, transaction records, Timesheets
- We do NOT store full credit/debit card numbers (tokenized by payment processors)

4.2 Information Collected Automatically

Device and Usage Information:

- Device type, model, operating system, unique device identifiers
- IP address, browser type and version
- Pages viewed, features used, time spent on Platform
- Log data (access times, error logs)

Location Data:

- GPS coordinates when clocking in/out of Shifts (to verify attendance)
- Approximate location from IP address (to show relevant Shifts)

Cookies and Similar Technologies:

- Session cookies (keep you logged in)
- Persistent cookies (remember preferences)
- Analytics cookies (usage patterns, performance monitoring)
- See Section 11 for full cookie policy

4.3 Information from Third Parties

Identity Verification Services:

- SingPass: Authentication data, citizenship verification
- Third-party KYC providers: Identity verification results, document authenticity

Payment Processors:

- Transaction confirmations, payment status, fraud detection signals
- We do NOT receive full card numbers (only tokenized references, last 4 digits)

Government Authorities (when required by law):

- Business registration data
- Publicly available professional information

4.4 Sensitive Personal Data

We collect Sensitive Personal Data ONLY when necessary and with explicit consent (or as permitted by law):

Health Data:

- Medical certificates for emergency cancellation documentation (voluntary)
- Medical documentation for Work Injury Compensation (WIC) claims (mandatory for claim processing under Platform Workers Act)
- Treatment records, hospital bills (for WIC claims only)
- Disability or medical conditions disclosed voluntarily (for workplace accommodations)

Biometric Data:

- Facial recognition from selfie with NRIC (for identity verification during registration)
- Retention: Deleted within 90 days after successful verification, UNLESS account flagged for fraud investigation (retained until investigation concludes + 1 year)
- NOT used for ongoing authentication, tracking, or profiling

Legal Basis for Processing Sensitive Personal Data:

- **Singapore:** Explicit consent, legal obligations (Platform Workers Act), insurance claims
- **EU/UK:** Explicit consent (GDPR Art. 9), legal claims, vital interests (medical emergencies)

---

5. HOW WE USE YOUR PERSONAL DATA

5.1 Primary Purposes

We Process your Personal Data for:

To Provide and Operate the Platform:

- Account creation, authentication, eligibility verification
- Matching Workers with Employers (skills, location, availability, ratings)
- Shift management (posting, browsing, booking, scheduling, tracking)
- Communication (messaging, notifications, reminders)
- Timekeeping and payment processing (clock-in/out, Timesheets, Escrow, transfers)
- Training platform access and certification tracking
- Ratings and reviews system

Legal Basis:

- Singapore: Consent (when you accept Terms)
- EU/UK: Performance of contract, Legitimate interests (operating marketplace)

Platform Workers Act Compliance (Workers in Singapore):

- Calculate and remit CPF MediSave contributions
- Report monthly earnings to CPF Board
- Administer Work Injury Compensation (WIC) claims
- Maintain compliance records for Ministry of Manpower (MOM)

Legal Basis:

- Singapore: Legal obligation (Platform Workers Act 2024)
- EU/UK: Legal obligation

To Ensure Trust, Safety, and Security:

- Identity verification (KYC), fraud prevention
- Anti-money laundering (AML) and counter-terrorism financing (CTF) compliance
- Platform integrity (detect Terms violations, abuse, harassment)
- Safety monitoring, injury report tracking
- Dispute resolution and Terms enforcement
- Security measures (protect against unauthorized access, cyberattacks)

Legal Basis:

- Singapore: Consent, Legal obligations (AML), Legitimate interests (fraud prevention)
- EU/UK: Legal obligations (AML/CTF), Legitimate interests (safety, security), Vital interests (emergencies)

To Process Payments and Financial Transactions:

- Escrow deposits, payment releases, withdrawals, refunds
- Financial recordkeeping, tax compliance
- Generate annual earning statements
- Anti-fraud transaction monitoring

Legal Basis:

- Singapore: Consent, Performance of contract, Legal obligations (tax)

- EU/UK: Performance of contract, Legal obligations (tax compliance)

To Improve and Personalize the Platform:

- Analytics and usage research
- Product development and feature improvement
- Personalized recommendations and Shift suggestions
- A/B testing and optimization
- We use aggregated and anonymized data (not identifiable) wherever possible

Legal Basis:

- Singapore: Consent, Legitimate interests (product improvement)
- EU/UK: Legitimate interests (improving services), Consent (where profiling has significant effects)

To Communicate with You:

- Service communications (account, Shifts, payments, policy changes)
- Customer support responses
- Notifications (push, SMS, email about Shifts, approvals, payments)
- Marketing communications (you can opt out—see Section 9.3)

Legal Basis:

- Singapore: Consent
- EU/UK: Performance of contract (service communications), Legitimate interests (support), Consent (marketing)

For Legal Compliance and Protection:

- Comply with laws, regulations, court orders, government requests
- Establish, exercise, defend legal claims
- Cooperate with law enforcement
- Internal audits and compliance monitoring

Legal Basis:

- Singapore: Legal obligations, Legitimate interests (legal claims)
- EU/UK: Legal obligations, Legitimate interests (legal defense), Vital interests (preventing harm)

5.2 Automated Decision-Making and Profiling

Shift Matching Algorithm:

- Automated ranking of Workers against Shift requirements
- Impact: Affects which Shifts you see, whether Employers see your profile
- Human Oversight: Employers make final selection

Fraud Detection:

- Machine learning models flag suspicious activity
- Impact: May result in account suspension pending manual review
- Human Oversight: All flagged accounts reviewed by staff before final action

Your Rights (EU/UK Users):

- Under GDPR Article 22, you have right NOT to be subject to decisions based solely on automated Processing with legal/significant effects
- We do NOT make fully automated decisions without human oversight
- You can request human review: privacy@joinflexi.work

---

6. HOW WE SHARE YOUR PERSONAL DATA

We do NOT sell your Personal Data to third parties.

We share Personal Data with:

6.1 Within the Platform (Employers and Workers)

Employers can see (about Workers):

- Profile information: Name, photo, ratings, reviews, skills, certifications, experience, languages
- Application details, Shift performance (attendance, punctuality, Timesheets)
- Reliability metrics (completion rate, response rate, cancellation rate)

Workers can see (about Employers):

- Company/business name
- Ratings and reviews from other Workers
- Shift postings with location details

NOT shared:

- Workers: Full NRIC, bank account, emergency contact, exact residential address, date of birth, health data
- Employers: Full financial details, internal business information

6.2 Service Providers and Data Processors

We share Personal Data with third-party service providers who Process data on our behalf under strict contractual obligations:

Payment Service Providers:

- MAS-licensed payment processors for Singapore operations
- Data Shared: Name, email, phone, bank account details, transaction amounts
- Purpose: Process Escrow deposits, payment releases, withdrawals, refunds, fraud detection
- Safeguards: Encryption, PCI DSS compliance, data processing agreements

Cloud Hosting and Infrastructure Providers:

- Secure cloud servers for Platform hosting and data storage
- Data Shared: All Platform data (stored on encrypted servers)
- Purpose: Host Platform, databases, backups; ensure scalability and reliability
- Location: Primary servers in Singapore; backups in secure data centers (Asia-Pacific)
- Safeguards: Encryption at rest and in transit, ISO 27001 certification, data processing agreements, Standard Contractual Clauses (SCCs) for EU/UK data

Identity Verification Services:

- SingPass (Singapore Government) and third-party KYC providers
- Data Shared: NRIC, passport, selfie photos, personal details
- Purpose: Verify identity, prevent fraud, ensure eligible users only
- Safeguards: SCCs, encryption, limited retention, data processed only for verification

Communication Services:

- SMS, email, and push notification providers
- Data Shared: Phone number, email address, device tokens, message content
- Purpose: Send notifications, alerts, reminders, support communications
- Safeguards: Encryption, data processing agreements

Analytics and Monitoring Tools:

- Usage analytics and error tracking services
- Data Shared: Usage data, device information, IP address (often anonymized)
- Purpose: Analyze Platform usage, identify bugs, improve performance
- Safeguards: Data anonymization where possible, SCCs, limited retention

Customer Support Tools:

- Support ticket and chat management platforms
- Data Shared: Name, email, support tickets, conversation history
- Purpose: Provide customer support, manage inquiries, resolve issues
- Safeguards: SCCs, encryption, access controls

Fraud Prevention and Security Services:

- Fraud detection and prevention platforms
- Data Shared: Account activity, transaction patterns, device fingerprints, IP addresses
- Purpose: Detect fraud, fake accounts, suspicious behavior
- Safeguards: SCCs, limited data sharing (only what's necessary)

All Service Providers:

- Contractually bound to Process Personal Data only for specified purposes
- Must implement appropriate security measures
- May not use data for their own purposes
- Required to comply with PDPA, GDPR, data protection laws
- Subject to audits and monitoring by FlexiWork

6.3 Business Transfers

In the event of merger, acquisition, sale of assets, bankruptcy, or insolvency:

- Your Personal Data may be transferred to successor entity as business asset
- We will notify you (email, Platform notice) before transfer
- Acquiring entity bound by this Privacy Policy (or provide comparable protections)
- You may delete your account before transfer if you do not wish data transferred

6.4 Government and Regulatory Authorities

We may disclose Personal Data to:

Singapore Authorities:

- **Central Provident Fund Board (CPF):**
    - Monthly contribution reports for all Workers (required under Platform Workers Act)
    - Data Shared: Worker name, NRIC, CPF account number, monthly earnings, contribution amounts
    - Purpose: Process mandatory CPF MediSave contributions
    - Frequency: Monthly automated reporting
- **Ministry of Manpower (MOM):**
    - Platform Workers Act compliance reporting
    - Work Injury Compensation (WIC) claims and incident reports
    - Data Shared: Worker details, injury circumstances, medical documentation, Shift records
    - Purpose: Administer WIC scheme, labor inspections, investigations
- **Inland Revenue Authority of Singapore (IRAS):**
    - Tax compliance, reporting (if legally required)
- **Monetary Authority of Singapore (MAS):**
    - AML/CTF compliance, financial regulations
- **Personal Data Protection Commission (PDPC):**
    - PDPA investigations or inquiries

EU/UK Authorities:

- UK Information Commissioner's Office (ICO), EU Data Protection Authorities (for GDPR compliance)

Law Enforcement and Courts:

- Singapore Police Force, law enforcement agencies (in response to valid legal process: subpoenas, court orders, warrants)
- Courts and tribunals (legal proceedings, arbitration, enforcement of rights)

When Disclosure Permitted/Required by Law:

- Comply with legal obligations
- Respond to lawful requests
- Establish, exercise, defend legal claims
- Protect our rights, property, safety, or that of users/public
- Prevent or investigate fraud, security breaches, illegal activity
- Emergencies involving risk of death or serious harm

We will notify you of legal requests unless:

- Prohibited by law or court order
- Notice would jeopardize investigation or public safety
- Emergency circumstances

6.5 With Your Consent

We may share Personal Data with third parties NOT listed above IF you provide explicit consent.

Examples:

- Sharing profile with partner platforms (opt-in)
- Displaying testimonials in marketing materials (with permission)
- Connecting account with third-party services you authorize

You can withdraw consent anytime (see Section 9.2).

6.6 Aggregated and Anonymized Data

We may share aggregated, anonymized, or de-identified data (that cannot identify you) with:

- Business partners, investors, potential acquirers
- Research institutions
- Public (in reports, blog posts)

This data does NOT constitute Personal Data as it cannot reasonably identify individuals.

---

7. INTERNATIONAL DATA TRANSFERS

7.1 Cross-Border Transfers

FlexiWork operates primarily in Singapore, but Personal Data may be transferred to, stored in, or accessed from countries outside Singapore, including:

- United States (payment processors, cloud hosting, analytics tools)
- European Union (cloud backups, support tools)
- Other Asia-Pacific countries (backup data centers, service providers)

Countries outside Singapore/EU/UK may have different data protection standards.

7.2 Safeguards for International Transfers

For Transfers from Singapore (PDPA):

- Contractual protections with service providers (PDPA-compliant clauses)
- Adequacy assessments of recipient countries' data protection laws
- Organizational safeguards (security measures, access controls)
- Your consent for transfers where required

For Transfers from EU/UK (GDPR/UK GDPR):

We use GDPR-compliant transfer mechanisms:

1. **Adequacy Decisions:** Transfers to countries recognized by EU Commission or UK Government as providing adequate protection

2. **Standard Contractual Clauses (SCCs):** EU Commission-approved contracts with service providers in countries without adequacy decisions (SCCs available upon request: privacy@joinflexi.work)

3. **Binding Corporate Rules (BCRs):** Some service providers have BCRs approved by EU authorities

4. **Additional Safeguards:**

    - Encryption of data in transit and at rest
    - Pseudonymization where feasible
    - Contractual obligations to challenge government data requests
    - Regular audits of service providers

7.3 Your Rights Regarding International Transfers

EU/UK Users:

- Right to obtain information about safeguards

- Can request copies of SCCs: privacy@joinflexi.work
- Can object to transfers if safeguards deemed inadequate (may affect service provision)

Singapore Users:

- Can withdraw consent for international transfers (may limit Platform functionality)

---

8. DATA RETENTION

8.1 Retention Principles

We retain Personal Data only as long as necessary for purposes collected, or as required by law.

Factors influencing retention:

- Legal and regulatory requirements
- Operational needs
- Legitimate interests (fraud prevention, legal claims)
- Contractual obligations
- Your consent (and whether withdrawn)

8.2 Specific Retention Periods

Data Category	Retention Period	Rationale
Account Information (name, NRIC, email, phone)	Account duration + 7 years after closure	PDPA/GDPR compliance; legal claims; financial recordkeeping
Identity Verification Documents (NRIC photos, selfies)	90 days after verification OR account closure + 7 years (if fraud prevention needed)	Minimize sensitive document retention; fraud prevention
CPF Contribution Records	7 years from contribution date	CPF Act requirements; Platform Workers Act compliance
Work Injury Compensation (WIC) Records	7 years from claim resolution	Platform Workers Act; legal claims; MOM requirements
Platform Workers Act Compliance Records (earnings, hours, contributions)	7 years from calendar year end	Statutory recordkeeping requirements

Transaction Records (payments, invoices, Timesheets)	7 years from transaction date	Singapore Companies Act, IRAS requirements, GDPR financial recordkeeping
Shift Data (postings, applications, Bookings, clock-in/out)	3 years from Shift completion	Operational needs; dispute resolution; analytics
Communications (Platform messages, support tickets)	3 years from last message	Customer support; dispute resolution; legal claims
Reviews and Ratings	Indefinitely (or until account deletion)	Transparency; trust & safety; informing future users
Dispute Records (evidence, determinations)	7 years from dispute resolution	Legal claims; arbitration records
Training Progress (certificates, quiz scores)	Account duration + 2 years	Operational needs; certificate verification
Analytics and Usage Data (aggregated/anonymized)	Indefinitely	Not Personal Data once anonymized
Cookies and Device IDs	13 months (session cookies deleted when browser closed)	EU ePrivacy Directive; analytics
Backup Data	90 days (rolling backups)	Disaster recovery; automatically overwritten

8.3 Retention After Account Deletion

When you close your account:

- **Immediate deletion:** Profile removed from public view; cannot log in
- **Retained for legal/regulatory compliance:** Transaction records, identity verification (if required for AML/fraud), dispute records (7 years)
- **Anonymization:** Where possible, data anonymized for analytics (no longer identifies you)
- **Backups:** Deleted data may remain in backups for up to 90 days (then automatically purged)

You can request expedited deletion (see Section 9.5), subject to legal retention requirements.

8.4 Inactive Accounts

If account inactive (no login) for:

- **24 months (Workers):** Reminders sent; after 36 months, account may be archived (data retained per schedule but account deactivated)
- **24 months (Employers):** Similar process; earlier deactivation if no Shifts posted for 12 months

You can reactivate by logging in (before data deletion periods expire).

---

9. DATA SECURITY

9.1 Security Measures

FlexiWork implements industry-standard technical and organizational measures to protect Personal Data:

Technical Safeguards:

- **Encryption:** TLS 1.2+ in transit, AES-256 at rest, field-level encryption for sensitive data (NRIC, bank accounts)
- **Access Controls:** Role-based access control (RBAC), principle of least privilege, multi-factor authentication (MFA) for employees, audit logs
- **Network Security:** Firewalls, intrusion detection/prevention systems, DDoS protection, secure API gateways
- **Application Security:** Secure coding practices, vulnerability scanning, penetration testing, regular security audits, patch management, input validation (protection against SQL injection, XSS, CSRF)
- **Data Minimization:** Collect only necessary data, pseudonymization where feasible

Organizational Safeguards:

- Employee training (mandatory data protection and security training, annual refreshers, confidentiality agreements)
- Background checks for employees with data access
- Data Protection Officer (DPO) / Data Protection Team (privacy@joinflexi.work)
- Incident response plan (documented procedures, regular drills)
- Vendor management (due diligence, data processing agreements, regular audits)
- Physical security (secure data centers with access controls, surveillance, ISO 27001/SOC 2 certifications)

9.2 Your Security Responsibilities

Account Security:

- Use strong, unique passwords (minimum 8 characters, mix of letters, numbers, symbols)

- Do NOT share password
- Enable Two-Factor Authentication (2FA) if available
- Log out after using shared/public devices
- Keep device secure (lock screen, antivirus, updated software)

Phishing Awareness:

- Be cautious of emails/messages claiming to be from FlexiWork asking for passwords or sensitive information
- We will NEVER ask for password via email or SMS
- Verify sender before clicking links (genuine emails from @joinflexi.work)
- Report suspicious emails: security@joinflexi.work

Monitor Your Account:

- Regularly review account activity, Shift history, payment transactions
- Report unauthorized activity immediately: security@joinflexi.work

9.3 Data Breach Notification

In the unlikely event of a data breach:

Notification to Authorities:

- **Singapore (PDPA):** Notify Personal Data Protection Commission (PDPC) within 72 hours if breach likely to result in significant harm
- **EU/UK (GDPR/UK GDPR):** Notify relevant Data Protection Authority (DPA) within 72 hours if breach affects EU/UK users

Notification to You:

- We will notify you without undue delay if breach likely to result in high risk to your rights and freedoms
- Notification includes: Nature of breach, affected data, likely consequences, measures taken, recommendations, contact point
- Method: Email, in-app notification, public notice on website (if unable to reach individuals)

9.4 Limitations

No system is 100% secure. Despite our best efforts, we cannot guarantee absolute security. You transmit data at your own risk.

If you believe your account compromised, contact immediately: security@joinflexi.work (24/7 monitoring)

---

10. YOUR RIGHTS AND CHOICES

10.1 Overview of Rights

Right	Singapore (PDPA)	EU/UK (GDPR/UK GDPR)
Access	✓	✓
Correction	✓	✓ (Rectification)
Erasure / Deletion	Limited	✓ ("Right to be Forgotten")
Restriction of Processing	Limited	✓
Data Portability	Limited	✓
Object to Processing	✓ (Withdrawal of consent)	✓
Withdraw Consent	✓	✓
Opt-Out of Marketing	✓	✓
Lodge Complaint	✓ (with PDPC)	✓ (with ICO/DPA)
Not Subject to Automated Decisions	Limited	✓

How to Exercise Rights: Email privacy@joinflexi.work with your request.

10.2 Right to Access (Data Subject Access Request)

You have the right to request:

- Confirmation of whether we Process your Personal Data
- Access to your Personal Data
- Information about how we Process your data

How to Request:

- Email: privacy@joinflexi.work
- Subject: "Data Access Request"
- Include: Full name, account email, NRIC (last 4 digits for verification)

What We Provide:

- Copy of Personal Data (PDF or CSV)
- Description of Processing activities

Timeline:

- Singapore: Within 30 days (may extend to 60 days for complex requests)
- EU/UK: Within 1 month (may extend to 3 months for complex requests)

Fees:

- First request: FREE
- Subsequent requests (if unfounded, excessive, repetitive): May charge reasonable fee (max SGD 50 / EUR 50) or refuse

10.3 Right to Correction / Rectification

You have the right to request correction of inaccurate or incomplete Personal Data.

How to Request:

- **Easy Update:** Most information can be updated directly in Account Settings
- **For Other Data:** Email privacy@joinflexi.work

We will correct inaccurate data within 30 days (Singapore) or 1 month (EU/UK).

We may refuse if:

- Correction would require altering factual records (e.g., historical Timesheets) where accuracy is disputed (refer to Dispute Resolution)
- Request is frivolous or excessive

10.4 Right to Erasure / Deletion ("Right to be Forgotten" - EU/UK)

You can request deletion of Personal Data in certain circumstances:

Grounds for Erasure (EU/UK GDPR):

- Personal Data no longer necessary for purposes collected
- You withdraw consent and there's no other legal basis
- You object to Processing and no overriding legitimate grounds
- Personal Data unlawfully Processed
- Erasure required for legal compliance

How to Request:

- Email: privacy@joinflexi.work
- Subject: "Data Deletion Request"

What We Will Do:

- Delete Personal Data where possible
- Anonymize data that must be retained for legal compliance
- Confirm deletion to you

Timeline: Within 30 days (Singapore) or 1 month (EU/UK)

Exceptions (We May Refuse or Limit Deletion If):

- Retention required by law (tax, financial: 7 years; legal claims: 6-7 years; Platform Workers Act: 7 years)
- Necessary for establishing, exercising, defending legal claims
- Necessary for compliance with legal obligation
- Outstanding payment disputes or legal proceedings

Singapore Note: PDPA does not explicitly provide "right to erasure," but you can withdraw consent (see Section 10.7). We will delete data not subject to legal retention requirements.

10.5 Right to Restriction of Processing (EU/UK)

You can request restriction (temporary suspension) of Processing in certain cases.

Grounds:

- You contest accuracy of Personal Data (restriction during verification)
- Processing is unlawful but you don't want erasure
- We no longer need data but you need it for legal claims
- You objected to Processing (restriction pending verification)

Effect: Data stored but not actively Processed (except with your consent or for legal claims)

How to Request: Email privacy@joinflexi.work with grounds

Timeline: Within 1 month (EU/UK)

Singapore Note: Not explicitly provided under PDPA; equivalent is withdrawing consent (see Section 10.7).

10.6 Right to Data Portability (EU/UK)

You can request a copy of Personal Data in structured, commonly used, machine-readable format (CSV, JSON).

Applies to:

- Data you provided to us
- Processing based on consent or contract
- Processing carried out by automated means

How to Request: Email privacy@joinflexi.work specifying format

What We Provide:

- Export of your data (account info, Shift history, Timesheets, payments, messages, training progress)
- Format: CSV or JSON

Timeline: Within 1 month (EU/UK)

Fee: FREE

Singapore Note: Not explicitly provided under PDPA; covered partially by Right to Access.

10.7 Right to Object / Withdraw Consent

Right to Object (EU/UK):

- You can object to Processing based on legitimate interests or direct marketing
- We must stop Processing unless we demonstrate compelling legitimate grounds (e.g., legal claims)

Withdrawal of Consent (Singapore & EU/UK):

- Where Processing based on consent, you can withdraw anytime
- Withdrawal does not affect lawfulness of Processing before withdrawal
- If you withdraw consent, we may be unable to provide certain services

How to Object/Withdraw:

- Email: privacy@joinflexi.work
- Specify which Processing activities you're objecting to

Marketing Opt-Out (easier method):

- Click "Unsubscribe" link in marketing emails
- Adjust preferences in Account Settings → Notifications
- Email: privacy@joinflexi.work (Subject: "Opt-Out of Marketing")
- We will process opt-out within 10 business days

10.8 Right to Lodge a Complaint

If you believe we violated your data protection rights:

Singapore:

- **Personal Data Protection Commission (PDPC)**
- Website: https://www.pdpc.gov.sg
- Email: info@pdpc.gov.sg
- Phone: +65 6377 3131

European Union:

- Lodge complaint with Data Protection Authority (DPA) in EU country where you reside, work, or where alleged infringement occurred
- Find your DPA: https://edpb.europa.eu/about-edpb/board/members_en

United Kingdom:

- **Information Commissioner's Office (ICO)**
- Website: https://ico.org.uk
- Helpline: 0303 123 1113
- Online: https://ico.org.uk/make-a-complaint/

We encourage you to contact us first (privacy@joinflexi.work) so we can address concerns directly.

10.9 Right Not to Be Subject to Automated Decision-Making (EU/UK)

You have right not to be subject to decisions based solely on automated Processing (including profiling) that produce legal effects or similarly significantly affect you.

Our Position:

- We use automated systems (Shift matching, fraud detection)
- Final decisions with significant effects involve human oversight
- No solely automated decisions with legal/significant effects without human review

If you believe an automated decision significantly affected you:

- Contact: privacy@joinflexi.work
- Request human review
- We will respond within 1 month

10.10 Verification and Fees

Identity Verification:

- To prevent unauthorized access, we may request additional information to verify identity
- Typically: Confirm account email, provide last 4 digits of NRIC, answer security questions

Fees:

- Most requests FREE
- May charge reasonable fee (max SGD 50 / EUR 50) for: Manifestly unfounded or excessive requests, repetitive requests
- May refuse excessive or unfounded requests

Response Timeline:

- 30 days (Singapore) or 1 month (EU/UK)
- May extend to 60 days / 3 months for complex requests (with notice)

---

11. CHILDREN'S PRIVACY

11.1 Age Restrictions

FlexiWork is NOT intended for children.

Minimum Age:

- Workers: 18 years old
- Employers: 18 years old (or 21 if required to enter contracts)

We do NOT knowingly collect Personal Data from individuals under 18.

11.2 Parental Rights

If you believe your child has provided Personal Data to FlexiWork:

- Contact immediately: privacy@joinflexi.work
- Provide: Child's name, account details, your relationship
- We will investigate and delete data if confirmed

---

12. COOKIES AND TRACKING TECHNOLOGIES

12.1 What Are Cookies?

Cookies are small text files stored on your device when you visit websites or use apps.

Similar Technologies: Web beacons, pixels, local storage, mobile SDKs

12.2 Types of Cookies We Use

Strictly Necessary Cookies:

- Purpose: Essential for Platform to function
- Examples: Session cookies, security cookies, load balancing
- Legal Basis: Legitimate interests (necessary for service); no consent required
- Cannot be disabled without breaking core features

Functional Cookies:

- Purpose: Remember preferences and settings
- Examples: Language preference, currency selection, "Remember Me"
- Legal Basis: Consent (implied by continued use)
- Can disable in browser settings

Analytics and Performance Cookies:

- Purpose: Understand user interaction, identify errors, improve performance
- Examples: Usage analytics, error tracking

- Data: Often anonymized or pseudonymized (IP addresses truncated)
- Legal Basis: Legitimate interests (product improvement); consent where required (EU/UK)
- Opt-Out: Disable in Cookie Settings or browser settings

Advertising and Marketing Cookies (if used):

- Purpose: Deliver relevant ads, measure effectiveness
- Legal Basis: Consent (required under GDPR/ePrivacy); opt-in required
- Opt-Out: Cookie Settings, browser settings, industry opt-out tools
- **Note:** We currently do NOT use advertising cookies, but may in future (with clear consent mechanisms)

12.3 Third-Party Cookies

Some cookies set by third-party services we use. We do not control these cookies—governed by third parties' privacy policies.

12.4 Cookie Duration

- **Session Cookies:** Deleted when browser closed
- **Persistent Cookies:** 13 months (EU ePrivacy standard) or shorter if specified
- **Strictly Necessary:** Varies (deleted after purpose fulfilled or session ends)

12.5 Managing Cookies

Cookie Settings on Our Platform:

- Click "Cookie Settings" link (footer of website)
- Choose which categories to accept (Strictly Necessary always enabled)
- Save preferences

Browser Settings:

- All browsers allow you to refuse or delete cookies
- Options: Block all cookies, block third-party cookies only, delete after each session

Mobile App Settings:

- iOS: Settings → Privacy → Tracking
- Android: Settings → Google → Ads → Opt out of Ads Personalization

Do Not Track (DNT):

- Some browsers offer DNT signals
- We currently do not respond to DNT signals (no universal standard)
- Use Cookie Settings or browser settings to manage tracking preferences

12.6 Consequences of Disabling Cookies

If you disable cookies:

- **Strictly Necessary:** Platform may not function (cannot log in, complete transactions)
- **Functional:** Lose personalized experience (language resets, preferences not saved)
- **Analytics:** No impact on your experience (we lose insights to improve Platform)
- **Advertising:** Fewer targeted ads (still see ads, just less relevant)

We recommend allowing at least Strictly Necessary and Functional cookies for best experience.

---

13. CHANGES TO THIS PRIVACY POLICY

13.1 Updates and Modifications

We may update this Privacy Policy to reflect:

- Changes in data practices
- New Platform features or services
- Changes in laws or regulations
- Feedback from users or regulators

13.2 Notice of Changes

We will notify you of material changes:

Method:

- Email to registered email address (at least 30 days before effective date for material changes)
- Prominent notice on Platform (banner, pop-up, login alert)
- Updated Privacy Policy posted at www.joinflexi.work/privacy
- "Last Updated" date at top updated

Material Changes include:

- New purposes for Processing Personal Data
- New categories of recipients
- Significant changes to your rights
- Changes to international transfer mechanisms
- Reduced data protection safeguards

Non-Material Changes (clarifications, formatting, minor updates):

- Posted on website without advance notice
- Continued use after effective date = acceptance

13.3 Your Choices Upon Changes

If you do not agree to updated Privacy Policy:

- You may stop using Platform
- You may close account before effective date (email: privacy@joinflexi.work)
- Continued use after effective date = acceptance of updated Privacy Policy

For EU/UK users: Material changes requiring new consent will prompt explicit consent mechanism (checkbox, opt-in) before taking effect.

13.4 Version History

Previous versions available for reference:

- www.joinflexi.work/privacy/history
- Or request via email: privacy@joinflexi.work

---

14. CONTACT INFORMATION AND DATA PROTECTION OFFICER

14.1 Contact Details

For privacy-related inquiries, requests, or complaints:

Email: privacy@joinflexi.work
(Monitored Mon-Fri, 9am-6pm SGT; responses within 3 business days)

Mail:
FlexiWork Pte. Ltd.
Attention: Data Protection Officer
60 Paya Lebar Road, #06-28
Paya Lebar Square
Singapore 409051

14.2 Data Protection Officer (DPO)

FlexiWork has appointed a Data Protection Officer responsible for:

- Overseeing PDPA, GDPR, UK GDPR compliance
- Monitoring data protection practices
- Conducting Data Protection Impact Assessments (DPIAs)
- Training staff on data protection
- Serving as point of contact for regulators and data subjects

DPO Contact: privacy@joinflexi.work

You can contact DPO directly regarding:

- Data protection concerns
- Exercising your rights
- Questions about this Privacy Policy
- Complaints about data handling

14.3 EU Representative (For GDPR Compliance)

For EU users, under GDPR Article 27, we may appoint an EU representative. Details will be provided here once appointed.

Until then, contact: privacy@joinflexi.work

14.4 Response Times

We aim to respond to inquiries within:

- General inquiries: 3-5 business days
- Data subject rights requests: 30 days (Singapore) / 1 month (EU/UK)
- Urgent security matters: 24 hours

---

15. SPECIFIC INFORMATION FOR EU/UK USERS

15.1 Legal Basis for Processing (GDPR/UK GDPR)

Under GDPR Article 6 and UK GDPR:

Processing Activity	Legal Basis
Account creation, Shift management, Payments	Performance of Contract (Art. 6(1)(b))
Identity verification (KYC), Fraud prevention, AML/CTF	Legal Obligation (Art. 6(1)(c)); Legitimate Interests (Art. 6(1)(f))
Platform improvement, Analytics, Personalization	Legitimate Interests (Art. 6(1)(f))
Marketing communications	Consent (Art. 6(1)(a))
Responding to legal requests, Legal claims	Legal Obligation (Art. 6(1)(c)); Legitimate Interests (Art. 6(1)(f))
Emergency situations (safety, injury)	Vital Interests (Art. 6(1)(d))
Platform Workers Act compliance (CPF, WIC)	Legal Obligation (Art. 6(1)(c))

For Sensitive Personal Data (GDPR Article 9):

- Explicit Consent (Art. 9(2)(a)) - e.g., health data for injury claims
- Legal Claims (Art. 9(2)(f)) - e.g., medical certificates for disputes
- Vital Interests (Art. 9(2)(c)) - e.g., emergency medical situations

15.2 Data Protection Impact Assessments (DPIAs)

We conduct DPIAs for high-risk Processing activities (large-scale profiling, processing sensitive data, automated decision-making).

DPIAs assess: Necessity and proportionality, risks to data subjects' rights, mitigation measures.

You can request summaries of DPIAs relevant to your data: privacy@joinflexi.work

15.3 UK-Specific Provisions

Following Brexit, UK GDPR applies to Processing of UK residents' data.

Differences from EU GDPR (minimal):

- Oversight by UK ICO (not EU DPAs)
- Adequacy decisions determined by UK Government
- UK-specific guidance from ICO
- Otherwise, protections are equivalent

UK Representative (if applicable): Details to be provided if required under UK GDPR Article 27.

---

16. SPECIFIC INFORMATION FOR SINGAPORE USERS

16.1 PDPA Compliance

FlexiWork complies with Singapore's Personal Data Protection Act 2012 (PDPA).

Key Points:

- **Consent:** By using Platform and accepting Terms, you provide consent for collection, use, disclosure of Personal Data as described
- **Purpose Limitation:** Personal Data collected only for purposes stated in Section 5
- **Withdrawal of Consent:** You can withdraw consent (see Section 10.7), subject to legal and contractual restrictions

16.2 Platform Workers Act 2024 Compliance

Statutory Obligations:

- FlexiWork must collect and process Worker earnings data to calculate and remit CPF MediSave contributions
- FlexiWork must report monthly to CPF Board and maintain records for 7 years
- FlexiWork must facilitate Work Injury Compensation (WIC) claims and share data with MOM
- These are legal obligations under Platform Workers Act 2024

Workers' Rights:

- You have right to access your CPF contribution records
- You can request correction of earnings data if inaccurate
- You cannot withdraw consent for Platform Workers Act compliance (statutory requirement)

16.3 Notification of Data Breaches (PDPA Amendment 2020)

Under PDPA (Amendment) 2020, we must notify PDPC and affected individuals of data breaches likely to result in significant harm.

Timeline: Within 72 hours of assessing that significant harm is likely.

What We Consider "Significant Harm":

- Unauthorized access to financial data (NRIC, bank accounts, credit cards)
- Large-scale data breach affecting many users
- Breach involving sensitive data (health, biometric)
- Risk of identity theft, financial loss, reputational damage

16.4 Do Not Call (DNC) Registry

Singapore's Do Not Call Registry protects individuals from unsolicited marketing messages.

Our Policy:

- We do NOT send marketing messages to numbers registered on DNC Registry (unless you explicitly consented or we have ongoing relationship)
- You can opt out of marketing anytime (see Section 10.7)
- To register your number on DNC: https://www.dnc.gov.sg

16.5 Cross-Border Data Transfers

Under PDPA Section 26, Personal Data transferred outside Singapore must receive comparable protection.

We ensure this through:

- Contractual safeguards with service providers
- Adequacy assessments of recipient countries
- Organizational measures (encryption, access controls)

You consent to international transfers as described in Section 7.

You can withdraw consent, though this may limit Platform functionality.

---

17. MISCELLANEOUS PROVISIONS

17.1 Third-Party Websites and Services

Platform may contain links to third-party websites, apps, or services.

We are NOT responsible for:

- Privacy practices of third parties
- Content or security of third-party sites
- Data collection by third parties

Third-party sites have their own privacy policies (please review before providing Personal Data).

17.2 California Privacy Rights (CCPA) - If Applicable

Currently, FlexiWork operates primarily in Singapore and does not specifically target California residents.

If we expand to serve California residents, we will comply with California Consumer Privacy Act (CCPA).

Contact for CCPA requests: privacy@joinflexi.work (Subject: "CCPA Request")

17.3 Conflict of Laws

If conflict between different legal requirements (e.g., PDPA vs. GDPR):

- We will apply strictest standard providing highest protection
- Comply with local law where you reside (if stricter)
- Seek legal guidance to resolve conflicts

Example: GDPR requires 1-month response to access requests; PDPA allows 30 days. We use stricter timeline (1 month) for all users for consistency.

17.4 Severability

If any provision invalid or unenforceable:

- That provision limited or eliminated to minimum extent necessary
- Remaining provisions remain in full force

17.5 Language

This Privacy Policy is drafted in English.

Translations may be provided for convenience.

In case of conflict, English version prevails.

17.6 Entire Agreement

This Privacy Policy, together with Terms & Conditions, constitutes entire agreement regarding Personal Data Processing.

Supersedes all prior privacy notices or statements.

---

18. ACKNOWLEDGMENT AND CONSENT

BY USING THE FLEXIWORK PLATFORM, YOU ACKNOWLEDGE AND CONSENT TO:

✓ **Reading and Understanding:** You have read and understood this Privacy Policy in its entirety

✓ **Collection and Processing:** FlexiWork may collect, use, disclose, and Process your Personal Data as described

✓ **International Transfers:** Your Personal Data may be transferred to, stored in, and Processed in countries outside Singapore/EU/UK with appropriate safeguards

✓ **Sharing with Third Parties:** Your Personal Data may be shared with service providers, Employers/Workers on Platform, government authorities, and other third parties as described

✓ **Platform Workers Act Compliance (Singapore Workers):** FlexiWork will collect earnings data, calculate and remit CPF MediSave contributions, report to CPF Board, and facilitate WIC claims as required by Platform Workers Act 2024

✓ **Automated Decision-Making:** Automated systems may be used for Shift matching and fraud detection (with human oversight for significant decisions)

✓ **Cookies and Tracking:** Cookies and similar technologies may be used to enhance user experience and analyze Platform usage

✓ **Changes to Privacy Policy:** This Privacy Policy may be updated from time to time; continued use after changes = acceptance

✓ **Your Rights:** You have rights regarding your Personal Data (access, correction, deletion, etc.) and can exercise them as described

✓ **Contact Us:** You can contact privacy@joinflexi.work for any privacy-related inquiries or concerns

✓ **Withdrawal of Consent:** You can withdraw consent at any time, subject to legal and contractual restrictions, though this may affect your ability to use Platform

FOR EU/UK USERS: Your consent is freely given, specific, informed, and unambiguous. You can withdraw consent at any time without affecting lawfulness of Processing before withdrawal.

FOR SINGAPORE USERS: By clicking "I Accept" on Terms & Conditions (which incorporate this Privacy Policy), you provide consent for collection, use, and disclosure of Personal Data as described.

LAST UPDATED: 11 January 2026
VERSION: 1.0
EFFECTIVE DATE: 11 January 2026

YOU HAVE REACHED THE END OF THE FLEXIWORK PRIVACY POLICY.

Questions or concerns about your privacy?

Contact us:

- **Email:** privacy@joinflexi.work
- **Mail:** FlexiWork Pte. Ltd., Attention: DPO, 60 Paya Lebar Road, #06-28, Paya Lebar Square, Singapore 409051

Thank you for trusting FlexiWork with your Personal Data. We are committed to protecting your privacy.

END OF PRIVACY POLICY