

## PAYMIT LIMITED - DATA PROTECTION & GDPR POLICY

### Contents

1.	Introduction .....	1
2.	What Data We Collect .....	1
a.	Customer Data .....	2
b.	Employee & Contractor Data .....	2
c.	Business Partner & Supplier Data .....	2
3.	How We Use Personal Data .....	2
a.	Providing Our Services .....	2
b.	Business Operations.....	2
c.	Marketing & Communication .....	2
4.	Legal Basis for Processing Personal Data .....	3
5.	Data Sharing & Disclosure .....	3
6.	International Data Transfers .....	3
7.	Data Retention & Secure Disposal .....	3
8.	Data Security Measures.....	4
9.	Individual Rights Under UK GDPR .....	4
10.	Data Breach Response.....	5
11.	Contact Information .....	5

### 1. Introduction

Paymit Ltd ("Paymit", "we", "our", "us") is committed to ensuring that personal data is collected, processed, stored, and handled in a secure and lawful manner. This policy outlines our data protection principles and compliance with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**.

The purpose of this policy is to:

- Ensure transparency in how we handle personal data.
- Establish guidelines for legal and ethical data processing.
- Inform individuals of their data rights and how to exercise them.
- Outline security measures we adopt to protect data.

This policy applies to all **customers, employees, suppliers, and third parties** who interact with Paymit Ltd.

### 2. What Data We Collect

We collect different types of personal data depending on our relationship with you.

#### **a. Customer Data**

- **Personal Information:** Name, Date of Birth, Nationality.
- **Contact Details:** Address, Phone Number, Email.
- **Identity & Verification Data:** Passport, Driving License, National ID, Proof of Address (Utility Bills, Bank Statements).
- **Financial & Transactional Data:** Bank Account Details, Source of Funds, Source of Wealth, Payment History, Geographic Location Data.

#### **b. Employee & Contractor Data**

- **Personal & Contact Information:** Name, Address, Email, Phone Number.
- **Employment Verification Data:** Right-to-Work documents (Biometric Resident Permit, Passport), Background Checks (DBS Reports).
- **Payroll & Contract Data:** Salary, National Insurance, Tax Contributions, Pension Details.

#### **c. Business Partner & Supplier Data**

- **Company Name & Registration Details.**
- **Regulatory Compliance Documents.**
- **Banking Information for Settlements & Payments.**

### **3. How We Use Personal Data**

We process personal data to fulfill our legal, contractual, and regulatory obligations.

#### **a. Providing Our Services**

- **Customer Identity Verification (KYC & AML Compliance).**
- **Processing Money Transfers & Currency Exchange Transactions.**
- **Preventing Fraud & Financial Crime (including sanction screening).**
- **Complying with FCA & HMRC requirements.**

#### **b. Business Operations**

- **Managing Customer Accounts & Inquiries.**
- **Maintaining Transaction & Compliance Records.**
- **Internal Audits & Reporting for Financial Oversight.**

#### **c. Marketing & Communication**

- **Sending service updates & transaction confirmations.**
- **Marketing campaigns, offers, and newsletters (only with consent).**
- **Customer satisfaction surveys & feedback collection.**

Paymit **never sells, rents, or trades** personal data.

#### 4. Legal Basis for Processing Personal Data

We process data under the following legal grounds:

- **Contractual Obligation:** To provide remittance & currency exchange services.
- **Legal Obligation:** Compliance with AML & KYC laws, HMRC & FCA regulations.
- **Legitimate Interest:** Fraud prevention, risk management, and service improvement.
- **Consent:** Marketing & promotional communication (opt-in required).

#### 5. Data Sharing & Disclosure

Paymit may share personal data **only where necessary** and in compliance with UK GDPR:

- **Regulators & Law Enforcement:** FCA, HMRC, National Crime Agency (NCA).
- **Payment Processing & Banking Partners:** For secure financial transactions.
- **Fraud Prevention & Credit Agencies:** To mitigate risks & comply with AML laws.
- **Cloud Storage & IT Providers:** For secure data storage & system operations.
- **Legal & Compliance Advisors:** For legal, tax, and regulatory obligations.

All third parties must comply with **Paymit's strict data protection standards**.

#### 6. International Data Transfers

In some cases, we may transfer personal data outside the UK/EEA, particularly for:

- **Processing international remittances.**
- **Compliance checks with international regulatory bodies.**
- **Data storage in secure cloud environments.**

We ensure data transfers are **lawful & secure** using:

- **Standard Contractual Clauses (SCCs) approved by UK GDPR.**
- **Transfers only to countries with adequate data protection laws.**
- **Encryption & access control for data security.**

#### 7. Data Retention & Secure Disposal

##### a. Data Retention Periods

Paymit Ltd retains data for the minimum period required by law, ensuring compliance with UK financial regulations and GDPR principles. We do **not** retain personal data longer than necessary.

- **Customer Data:** Retained for **five (5) years after the conclusion of the business relationship**, as required under the **Money Laundering Regulations (MLR) 2017**.
- **Employee Records:** Retained for **six (6) years after the termination of employment**, as required for tax and legal compliance.
- **Transaction & Compliance Reports (AML & SARs):** Retained for **six (6) years**, in line with FCA and HMRC regulations.
- **Marketing Data:** Retained **until consent is withdrawn** or after a period of inactivity, as per GDPR consent rules.

#### **b. Secure Data Deletion & Disposal**

Once the retention period expires, Paymit ensures that data is **securely and permanently deleted** to prevent unauthorized access or misuse. The following measures are applied:

- **Digital Data Disposal:** Encrypted deletion protocols and **certified data erasure** software are used to remove all records from Paymit's systems, ensuring irreversibility.
- **Physical Document Disposal:** Any printed or physical records are **shredded using industrial-grade shredders** and disposed of in compliance with UK data protection laws.
- **System Logs & Backups:** Data backups are systematically **wiped** once the required retention period has elapsed, ensuring that no residual information remains accessible.

### **8. Data Security Measures**

Paymit Ltd applies **stringent security controls** to protect all personal data.


- **Encryption:** All stored and transmitted data is encrypted.
- **Access Controls:** Only authorized personnel with a need-to-know basis can access sensitive data.
- **Two-Factor Authentication (2FA):** Mandatory for both internal staff and customer logins.
- **Firewall & Intrusion Detection Systems (IDS):** Constant monitoring of network security.
- **Regular Security Audits:** Periodic penetration testing and vulnerability assessments.
- **Employee Cybersecurity Training:** Staff undergo **mandatory annual GDPR and data protection training**.

### **9. Individual Rights Under UK GDPR**

Under UK GDPR, individuals have the right to:

1. **Access Personal Data** – Request a copy of your personal information.
2. **Request Rectification** – Correct inaccurate or incomplete data.
3. **Request Erasure ("Right to be Forgotten")** – Request deletion under specific conditions.

4. **Restrict Processing** – Limit how we use your data in certain situations.
5. **Data Portability** – Receive your data in a structured format for reuse.
6. **Object to Processing** – Prevent your data from being used for marketing.
7. **Withdraw Consent** – Opt out of marketing communications at any time.
8. **Lodge a Complaint** – If you believe your data rights have been violated, you can complain to the **ICO (Information Commissioner's Office)**.

 **To exercise these rights, contact:** [info@paymit.co.uk](mailto:info@paymit.co.uk)

---

## 10. Data Breach Response


If a **data breach** occurs:


1. **Assessment & Containment:** Immediate risk analysis and mitigation steps are taken.
2. **Notification to Authorities:** If the breach poses a high risk, Paymit **notifies the ICO within 72 hours**.
3. **User Notification:** If the breach affects individuals, impacted users are informed.
4. **Preventative Measures:** Further security enhancements are implemented to prevent recurrence.

## 11. Contact Information

For inquiries regarding this policy:

 **Email:** [info@paymit.co.uk](mailto:info@paymit.co.uk)

 **Address:** 85 Great Portland Street, First Floor, London, England, W1W 7LT

 **Complaints:** Visit [ICO's website](#)

## 12. Updates to This Policy

This policy is reviewed annually or upon regulatory changes. Any updates will be published on our website.

 **Last Updated:** March 2025

## Acknowledgment & Consent

By using our services, you acknowledge and agree to this policy.

**Paymit Ltd ensures full compliance with UK GDPR to protect your personal data.**