

Data Processing Agreement

MySalaryPal Ltd — Version 1.0 — Issued 09 June 2026

This Data Processing Agreement ("DPA") forms part of the agreement between MySalaryPal Ltd ("Processor") and the customer entity identified in the order form ("Controller") for the MySalaryPal payroll platform (the "Service"). It reflects the parties' obligations under the EU General Data Protection Regulation 2016/679 ("GDPR"), the UK GDPR and the Irish Data Protection Act 2018.

1. Subject matter and duration

The Processor will process personal data on behalf of the Controller solely for the purpose of providing the Service for the duration of the master subscription agreement. This DPA terminates automatically when the underlying subscription ends.

2. Nature and purpose of processing

Storage, transmission, organisation, retrieval, consultation, restriction, erasure and destruction of personal data necessary to operate a multi-country payroll portal, including payslip delivery, leave, expenses, RAMS, training records, audit logging and notifications.

3. Categories of data subjects

Employees, contractors, directors, payroll administrators and other authorised users of the Controller. Categories of personal data include: identifiers (name, email, employee ID, address), financial data (bank details, salary, tax codes, payslip data), employment data (department, role, manager, start/end dates), special-category data only where the Controller explicitly uploads it (e.g. trade-union or health information attached to leave requests) and technical data (IP address, device, audit timestamps).

4. Controller and Processor obligations

The Controller warrants it has a lawful basis to process the personal data and to instruct the Processor. The Processor will:

- Process personal data only on documented instructions from the Controller (including those provided through the Service's standard configuration).
- Ensure persons authorised to process the personal data are bound by confidentiality.
- Implement the technical and organisational measures set out in Annex II.
- Assist the Controller, taking into account the nature of processing, to fulfil data subject requests and Articles 32–36 GDPR obligations.
- Make available all information necessary to demonstrate compliance and allow for audits, including inspections, conducted by the Controller or another auditor mandated by the Controller (subject to reasonable notice and confidentiality).
- At the choice of the Controller, delete or return all personal data after the end of the provision of services and delete existing copies unless EU or Member State law requires storage.

5. Sub-processors

The Controller grants general authorisation for the Processor to engage the sub-processors listed at <https://mysalarypal.com/trust>. The Processor will give at least 30 days' notice of any intended change. The Controller may object on reasonable grounds related to data protection within that period; if the parties

cannot agree a resolution, either party may terminate the affected service.

6. International transfers

Personal data is hosted in the European Union (Frankfurt, Germany). Where a sub-processor processes data outside the EEA, the Processor relies on (a) European Commission adequacy decisions where available, or (b) the 2021 Standard Contractual Clauses (Module 3) with supplementary technical measures including encryption at rest and in transit.

7. Personal data breach notification

The Processor will notify the Controller without undue delay and in any event within 72 hours of becoming aware of a personal data breach affecting the Controller's data. Notification will include the nature of the breach, categories and approximate number of data subjects, likely consequences and measures taken or proposed.

8. Liability and term

Liability under this DPA is governed by the limitation of liability clause of the master subscription agreement. This DPA prevails over conflicting provisions of the master agreement with respect to data protection.

Annex I — Description of the transfer

Data exporter	The Controller identified on the order form.
Data importer	MySalaryPal Ltd, Dublin, Ireland.
Categories of data subjects	Employees, contractors and admin users of the Controller.
Categories of personal data	Identifiers, employment, payroll, financial, technical.
Special categories	Only if uploaded by the Controller (e.g. health attached to leave).
Frequency	Continuous, for the duration of the subscription.
Nature of processing	Hosting, organising, retrieving, deleting, transmitting.
Purpose	Operation of the MySalaryPal multi-country payroll platform.
Retention	For the duration of the subscription + 12 months, then deleted.

Annex II — Technical and organisational measures

Encryption	TLS 1.2+ in transit. AES-256 at rest for database, file storage and backups.
Access control	Role-based access enforced at the database layer (RLS). MFA required for all production access.
Authentication	Email + password with HIBP leaked-password check, Google OAuth, SAML SSO, WebAuthn passkeys.
Network security	Edge protection via Cloudflare. Rate limiting on auth and write endpoints.
Backups	Encrypted daily backups, 30-day point-in-time recovery.
Logging & monitoring	Tamper-evident audit log of admin actions, payslip views, exports and policy changes.
Personnel	Confidentiality obligations, background checks where lawful, security training on hire and annually.
Vendor management	Sub-processors reviewed before engagement and on material change.
Incident response	Documented playbook; 72-hour controller notification.
Data segregation	Logical separation per workspace and per group; cross-tenant reads blocked at policy layer.
Deletion	Self-service data export and erasure. Hard delete on subscription termination.

Signed for and on behalf of the parties

MySalaryPal Ltd (Processor)	Customer (Controller)
Name:	Name:
Title:	Title:
Date:	Date:

Signature:

Signature: