Data Processing Agreement

Direct customers · Version 2.1 · Effective 6 November 2026

This Data Processing Agreement ("DPA") is incorporated into the Order Form and the MSA between AIPayroll Limited (trading as "Flow Payroll", the "Supplier") and the Client identified in the Order Form (the "Client"). It governs the processing of personal data in connection with the Services.

1) Definitions

The terms controller, processor, sub-processor, data subject, personal data, personal data breach and processing have the meanings given in the UK GDPR. Capitalised terms used but not defined in this DPA have the meanings given in the MSA. In addition:

a) **Applicable Data Protection Law:** the UK GDPR, the Data Protection Act 2018 and, to the extent applicable, the EU GDPR, together with all related laws in force from time to time.

b) **UK GDPR:** has the meaning given in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018.

c) **Payee Data:** personal data relating to the employees and workers of the Client, processed through the Services for payroll purposes.

d) **Standard Contractual Clauses:** the EU standard contractual clauses approved by Commission Implementing Decision (EU) 2021/914 and the UK International Data Transfer Addendum to them, and/or such other transfer mechanism approved under Applicable Data Protection Law.

2) Roles of the Parties

a) In respect of Payee Data processed through the Services, the Client (as employer) is the controller and the Supplier (Flow) is the processor, processing Payee Data on the documented instructions of the Client.

b) The Client warrants that it has a lawful basis for the processing under this DPA and has provided, and will continue to provide, its Payees with all privacy information required in respect of that processing, including the Supplier's processing as processor.

c) In respect of the Client's own business contact data (e.g. Authorised User account data), the Client is controller and the Supplier is processor, save to the extent the Supplier processes such data as controller for its own purposes (including account administration, security, billing and service improvement) in accordance with its Privacy Policy, and the remainder of this DPA applies accordingly.

d) If the roles determined in this clause change, the parties will work together in good faith to make any necessary changes to this DPA.

3) Instructions and Compliance

a) The Supplier shall process personal data only on the documented instructions of the Client, as set out in this DPA and the Agreement, unless required by Applicable Laws to do otherwise (in which case it shall notify the Client unless prohibited by law). The Client shall ensure that all instructions are complete, accurate and lawful.

b) The Supplier shall promptly inform the Client if, in its opinion, an instruction infringes Applicable Data Protection Law.

c) Both parties shall comply with their respective obligations under Applicable Data Protection Law. Each party shall ensure it has a lawful basis and all necessary notices and consents for the processing it directs or performs.

d) The Client shall indemnify the Supplier against all losses, fines and costs arising from any instruction given by the Client that infringes Applicable Data Protection Law, or any failure by the Client to have a lawful basis for, or to provide the privacy information required in respect of, the processing under this DPA.

4) Supplier's Obligations

In relation to personal data it processes, the Supplier shall:

a) implement appropriate technical and organisational measures to protect against unauthorised or unlawful processing and accidental loss, destruction or damage (see Annex 2);

b) ensure personnel authorised to process the data are bound by confidentiality and are appropriately trained;

c) assist the Client in responding to data-subject requests and in complying with security, breach-notification, DPIA and regulator-consultation obligations, using

the Supplier's standard export and support functionality (the Supplier may charge its reasonable costs for non-standard or high-volume assistance);

d) notify the Client without undue delay and in any event within 24 hours of becoming aware of a personal data breach involving the data, with sufficient information to enable the Client to meet its own notification obligations;

e) on the Client's written direction, delete or return the data on termination, save where retention is required by Applicable Laws (see clause 7); and

f) maintain records demonstrating compliance with this DPA, and make available information reasonably necessary to demonstrate compliance.

5) Sub-Processing

a) The Client provides general authorisation for the Supplier to appoint sub-processors, including those listed in Annex 3, provided that any transfer outside the UK or EEA complies with clause 6(b), and provided the Supplier: (i) imposes data-protection terms on each sub-processor equivalent to those in this DPA; (ii) remains liable to the extent required by Applicable Data Protection Law for their acts and omissions; and (iii) maintains a list of sub-processors (Annex 3) and gives the Client at least 30 days' notice of any intended addition or replacement.

b) The Client may object to a new sub-processor on reasonable data-protection grounds within the notice period. Where the Client's reasonable concerns remain unresolved following good-faith discussion and the Supplier has been unable, within 30 days of the objection, to offer a reasonable alternative, the Client may terminate the affected Services without penalty.

6) International Transfers

a) The Supplier's hosting infrastructure is located within the United Kingdom and the European Economic Area, with the primary environment in Amazon Web Services' Europe (Ireland) region and a secondary environment in the Europe (London) region. Transfers between the Supplier's EEA and UK environments are made in reliance on the applicable adequacy findings.

b) Where the Supplier transfers personal data outside the UK (including access by personnel or sub-processors located outside the UK), it shall ensure the transfer is effected under a valid transfer mechanism under Applicable Data Protection Law, including the Standard Contractual Clauses / UK International Data Transfer Addendum, or reliance on an adequacy decision.

c) The Client shall promptly comply with any reasonable request of the Supplier to enter into such Standard Contractual Clauses as are required to legitimise a transfer.

7) Retention and Return

a) The Supplier shall process Payee Data for the term of the Agreement and shall retain, return and delete it, during and after the term, in accordance with the Data Retention Schedule.

b) Before deleting or returning Payee Data, the Supplier shall give the Client a reasonable opportunity and period to export the data using the Supplier's standard export functionality.

c) On termination or expiry, the Supplier shall return or delete the Payee Data in accordance with the Data Retention Schedule, save where retention is required by Applicable Law. Where deletion is not technically feasible (for example, routine backups pending overwrite), the Supplier shall put the data beyond further use and delete it as backups are cycled and overwritten, in any event within 35 days.

8) Audit

a) The Supplier shall make available, on reasonable request and no more than once per year (unless required by a regulator or following a personal data breach), such information as is reasonably necessary to demonstrate compliance with this DPA.

b) The Supplier's primary method of demonstrating compliance shall be written assurance materials prepared or held by the Supplier, which may include the independent audit reports and certifications held by its infrastructure and sub-processors, and evidence of the Supplier's own technical and organisational measures. Such materials will be provided at no charge.

c) Where the assurance materials are reasonably insufficient, or a personal data breach affecting the Payee Data has occurred, the Client (or its independent auditor, who is not a competitor of the Supplier and is subject to reasonable confidentiality obligations) may, on at least 30 days' notice and no more than once in any 12-month period (save following a personal data breach) and during business hours, conduct a further audit limited to what is reasonably necessary to verify compliance. Audits are at the Client's cost, save where they reveal a material breach of this DPA by the Supplier.

9) Liability

a) The Supplier's total aggregate liability arising out of or in connection with this DPA shall not exceed £500,000 (the "DPA Cap"), aggregated with the Supplier's liability under clause 12.4 of the MSA in accordance with clause 12.9 of the MSA. Nothing in this DPA limits the Client's liability.

Annex 1 — Particulars of Processing

Subject matter	Provision of UK payroll software services to the Client.
Nature & purpose	Processing of Payee Data to calculate pay, tax, National Insurance, pension contributions and deductions; generate payslips; make RTI and pension submissions; produce year-end outputs; hosting, storage and back-up; providing support; security monitoring and incident response (including the use of AI tooling as described in Annex 3); product analytics using pseudonymised data; and creating anonymised and aggregated data in accordance with clause 10.5 of the MSA.
Duration	The term of the Agreement, plus the retention period in the Data Retention Schedule (see clause 7).
Types of personal data	Name, address, date of birth, gender, National Insurance number, tax details, employment details, pay, benefits, deductions, contributions and taxes, pension enrolments; optionally bank account details, email address and telephone number.
Special category data	Data concerning health (e.g. statutory sick, maternity, paternity and adoption pay) and trade union membership (e.g. subscription deductions), to the extent required for payroll.
Categories of data subject	The employees and workers ("Payees") of the Client; and the Client's Authorised Users.
Controllers	The Client, in respect of its Payee Data and its Authorised User data.
Processor	The Supplier (Flow), as processor.

Annex 2 — Technical and Organisational Measures

The Supplier maintains, at a minimum, the following measures, which may be updated, replaced or enhanced from time to time provided overall security is not materially diminished:

- Encryption of personal data at rest and in transit;
- Hosting on AWS with access controls and network segregation;
- Role-based access control and least-privilege principles for personnel;
- Logging, monitoring and alerting on access to personal data;
- Regular backups and a documented business-continuity / disaster-recovery process;
- Vulnerability management, patching and periodic penetration testing;
- Personnel confidentiality undertakings and data-protection training; and
- An incident-response process supporting breach notification within 24 hours.

Annex 3 — Sub-Processors

The Supplier's current sub-processors are listed below. This list forms part of this DPA and will be updated by notice to the Client in accordance with clause 5(a).

Sub-processor	Purpose	Location
Amazon Web Services, Inc. (AWS)	Cloud hosting and infrastructure provider. The Supplier's application and databases are hosted on AWS.	European Union (Ireland)
PostHog, Inc.	Product analytics used to understand feature usage and application performance. Data is pseudonymised, anonymised or aggregated.	European Union (Germany)
Postmark (ActiveCampaign, LLC)	Transactional email delivery for application notifications (e.g. account invites, password resets).	European Union
Anthropic, PBC	Large-language-model inference supporting the Supplier's internal operational and incident-response tooling and, in future, AI-assisted product features. The Supplier applies data minimisation so that identifiable Payee Data is not deliberately provided to Anthropic; in rare cases an identifier may appear incidentally in an error log. Inputs and outputs are not used to train Anthropic's models.	United States (transfers under SCCs / UK Addendum)