Data Processing Agreement

FMOps DPA v1.0 — August 2026 — template; the signed copy for each engagement is issued at contract stage.

This agreement is made under Article 28 of Regulation (EU) 2016/679 (the GDPR). It sets out how FMOps handles personal data when it processes that data on behalf of the Client.

1. Parties

ROLE	PROCESSOR	CONTROLLER
Name	Fionn Murphy, sole trader trading as FMOps	The Client, as named in the Services Agreement
Address	Waterford, Ireland	As named in the Services Agreement
Contact	fionn@fmops.ie · +353 86 107 2373	As named in the Services Agreement

FMOps is referred to below as "the Processor" or "I". The Client is referred to as "the Controller" or "you". This agreement is additional to, and forms part of, the written quote, order confirmation or services contract between us (the "Services Agreement").

2. Definitions

- **Personal data, processing, controller, processor, data subject, personal data breach** have the meanings given in Article 4 of the GDPR.
- **Data Protection Law** means the GDPR, the Irish Data Protection Act 2018, and any other data protection law that applies to the processing.
- **Services** means the work described in the Services Agreement: a Claude for Small Business install, an automation build, a website, an AI search visibility service, or support for any of these.
- **Sub-processor** means another processor engaged by the Processor to carry out processing activities on behalf of the Controller.
- **Your Systems** means the accounts and tools the Controller owns or licenses, for example Google Workspace, Microsoft 365, an accounts package, or a Claude for Work workspace held in the Controller's own name.

3. Subject matter, duration, nature and purpose of processing

3.1 Subject matter

The Processor processes personal data only so far as needed to deliver the Services. In most engagements this means working inside Your Systems to set up, configure, test, document and support connections and workflows. The Processor does not build a separate copy of the Controller's data.

3.2 Nature of the processing

- Access to named accounts, mailboxes, folders and records under scoped permissions, to configure and test the Services.
- Viewing sample records or messages while testing a workflow on a real case.
- Configuring, running and checking automated workflows that the Controller has approved.
- Reproducing and fixing a fault reported by the Controller during support.

The Processor does not copy, export, download or keep the Controller's personal data on FMOps systems, except for a short-lived working note or screenshot needed to fix a specific fault, which is deleted when that fault is closed.

3.3 Purpose

The only purpose is delivery and support of the Services under the Controller's documented instructions. The Processor does not use the Controller's personal data for its own purposes, for marketing, for benchmarking, or to

train any AI model.

3.4 Duration

Processing starts when access is first granted and ends at the earlier of: the end of the Services Agreement, or the point at which all Processor access has been removed. Setup access is removed at handover. Where the Controller keeps a monthly support plan, access is granted per job and removed when that job is closed, and each grant and removal is logged.

4. Categories of data and data subjects

The types of personal data and the categories of data subject are set out in Annex 1. Before any account is connected, we agree in writing which categories of data may be used in workflows and which are excluded. Payroll data and health data are commonly excluded. Annex 1 records that decision for this engagement.

5. Processor obligations

5.1 Documented instructions

The Processor processes personal data only on the documented instructions of the Controller. This agreement, the Services Agreement, the written connection list produced at handover, and any later written instruction from the Controller together form those instructions. If the Processor believes an instruction breaches Data Protection Law, the Processor tells the Controller without delay and may pause that part of the work.

5.2 Confidentiality

The Processor keeps all personal data confidential and uses it only for the Services. FMOps is a one-person business: no employee, contractor or other person is given access to the Controller's data or accounts. If that ever changes, any person given access will be bound in writing by confidentiality duties at least as strict as these, and the Controller will be told first.

5.3 Security

The Processor puts in place appropriate technical and organisational measures under Article 32 of the GDPR. The measures in force are listed in Annex 2. The Processor reviews them at least once a year and may replace a measure with one that is at least as protective.

5.4 Sub-processors

The Controller gives general written authorisation for the Processor to engage sub-processors. The current list is in Annex 3. The Processor gives the Controller at least 14 days' written notice before adding or replacing a sub-processor that will process the Controller's personal data. The Controller may object on reasonable data protection grounds within that period; if the objection cannot be resolved, either side may end the affected part of the Services under the Services Agreement, with no penalty for the Controller.

The Processor imposes on each sub-processor, by written contract, data protection obligations equivalent to those in this agreement, and remains liable to the Controller for the sub-processor's performance.

Where the Controller contracts a provider directly — for example Anthropic for Claude licences, or Google or Microsoft for the Controller's own email suite — that provider is the Controller's own processor, not a sub-processor of FMOps. Anthropic's own Data Processing Addendum covers what Anthropic does with content sent to Claude.

5.5 Assistance with data subject requests

If the Processor receives a request from a data subject about the Controller's data, the Processor does not answer it directly. The Processor forwards it to the Controller within 2 working days and helps the Controller answer it. Help includes locating data in a connected system, explaining what a workflow did with a record, and exporting or deleting a record on the Controller's written instruction. This assistance is included in the Services at no extra charge unless the volume of requests makes it unreasonable, in which case time is quoted in advance.

5.6 Assistance with Articles 32 to 36

The Processor gives the Controller reasonable help, taking account of the nature of the processing and the information available to the Processor, with:

- keeping processing secure (Article 32);

- notifying a personal data breach to the supervisory authority and to data subjects (Articles 33 and 34);
- carrying out a data protection impact assessment (Article 35); and
- prior consultation with the supervisory authority (Article 36).

5.7 Deletion and return at the end of the Services

At the end of the Services, or sooner on the Controller's written request, the Processor:

- removes its own access to all of Your Systems, and hands the Controller the admin role on any workspace set up for the Controller;
- gives the Controller a written note of every connection made and how to disconnect it;
- deletes any working copy, note, screenshot or export that holds the Controller's personal data, or returns it first if the Controller asks in writing; and
- confirms deletion in writing on request.

The Processor may keep records it must keep by law — for example invoices and tax records, which Irish Revenue requires to be kept for 6 years. Those records are kept only for that purpose and stay subject to clauses 5.2 and 5.3.

5.8 Audits and information

The Processor makes available to the Controller all information reasonably needed to show that this agreement is being met, and allows and contributes to audits and inspections by the Controller or an auditor the Controller appoints. Audits are on at least 21 days' written notice, during normal working hours, no more than once a year unless a breach or a supervisory authority requires more, and must not disclose another client's confidential data. The Controller bears the cost of an audit it initiates.

6. International transfers

The Processor is based in Ireland. Where FMOps holds project records, those records are held in the European Union: the FMOps database is hosted by Supabase in its EU (Ireland) region, and site hosting is provided by Vercel.

The Controller's own business data stays in Your Systems, under the data-location terms the Controller already has with those providers. A Claude install does not move that data into a new system.

Where a sub-processor is established outside the European Economic Area, or processes personal data outside the EEA, the transfer relies on one of the following:

- an adequacy decision of the European Commission, including the EU–US Data Privacy Framework where the provider is certified under it; or
- the European Commission's Standard Contractual Clauses (Decision 2021/914), module three (processor to processor), with the transfer impact assessment and any additional measures the case requires.

Annex 3 records, for each sub-processor, where processing takes place and which transfer mechanism applies. The Processor does not make a new transfer outside the EEA without a lawful mechanism in place first.

7. Personal data breach notification

The Processor notifies the Controller in writing without undue delay, and in any case within 48 hours, of becoming aware of a personal data breach affecting the Controller's personal data. The notification includes, so far as known at the time:

- what happened and when it was discovered;
- the categories and approximate number of data subjects and records affected;
- the likely consequences;
- the measures taken or proposed to deal with it and to limit harm; and
- a contact point for further information.

Where the full picture is not available within 48 hours, the Processor sends what is known and follows up in stages without further undue delay. The Processor does not notify a supervisory authority or a data subject on the Controller's behalf unless the Controller instructs it in writing.

8. Liability

Liability under this agreement is governed by, and subject to, the limits and exclusions of liability in the Services Agreement, which apply as if set out here in full. Nothing in this agreement limits liability that cannot be limited by law, and nothing in it limits a data subject's rights under Article 82 of the GDPR.

9. General

- **Order of precedence.** If this agreement conflicts with the Services Agreement on a data protection matter, this agreement wins on that matter. On all other matters the Services Agreement wins.
- **Changes.** A change to this agreement is valid only if both parties agree it in writing. The Processor may update Annex 2 to add or improve a security measure, and updates Annex 3 under clause 5.4.
- **Term.** This agreement runs for as long as the Processor processes personal data for the Controller. Clauses 5.2, 5.7, 6 and 8 survive its end.

10. Governing law

This agreement is governed by the law of Ireland. The courts of Ireland have exclusive jurisdiction over any dispute arising from it.

11. Signatures

Signed by the authorised representatives of both parties.

Processor — FMOps

Signature

Name: Fionn Murphy, trading as FMOps

Date

Controller — the Client

Signature

Name and position

Date

Annex 1 — Data and data subjects

Completed for each engagement before any account is connected.

Categories of data subject

IN SCOPE	CATEGORY
☐	The Controller's customers and prospective customers
☐	The Controller's staff, as senders and recipients of business email
☐	The Controller's suppliers and contractors
☐	Other (write in):

Types of personal data

IN SCOPE	TYPE
☐	Names and job titles
☐	Business contact details: email, phone, postal address
☐	Content of business email and messages
☐	Documents and files in connected folders
☐	Quotes, orders, invoices and payment status
☐	Appointment and job records
☐	Other (write in):

Excluded categories

The following are not to be used in any workflow, and no connection is made that exposes them:

EXCLUDED	CATEGORY
☐	Special category data under Article 9 of the GDPR, including health data
☐	Payroll data and employee records
☐	Criminal offence data
☐	Payment card and full bank details
☐	Data about anyone under 18
☐	Other (write in):

Connections

The written connection list produced at handover forms part of this Annex: it records each connected account, the scope granted (read-only or write), the purpose, and how to disconnect it.

Annex 2 — Security measures (Article 32)

Access control

- Access is granted under a named FMOps account, never a shared login, and never a staff member's personal account.
- Access is read-only where read-only is enough, and limited to the folders, mailboxes and records the work needs.
- Multi-factor authentication is on for every FMOps account used in the work, including the FMOps Google Workspace account.
- Passwords are unique per service and held in a password manager. Nothing is written down in plain text.

- Setup access is removed at handover. Support access is granted per job and removed when the job is closed. Each grant and removal is logged with a date.

Device security

- Work devices use full-disk encryption, an automatic screen lock, and an operating system that still receives security updates.
- Devices are kept patched. Remote wipe is enabled.

Data minimisation

- The Controller's personal data is not copied, exported or stored on FMOps systems.
- Where a short-lived working note or screenshot is needed to fix a fault, it holds the minimum data required and is deleted when the fault is closed.
- Test workflows use the Controller's own live case only with the Controller's agreement, and never move data outside the connected systems.

Workflow safeguards

- Any workflow that sends an email or message, issues an invoice, changes a record or moves money stops for a named person to approve, unless the Controller asks in writing to remove that step.
- No decision with a legal or similarly significant effect on a person is made by automated processing alone (Article 22).
- API keys and credentials are held in the Controller's own accounts or in the platform's secret store, never in code, email or chat.

Transmission and storage

- All connections use TLS. Files are shared by permissioned link inside the Controller's own systems rather than as email attachments.
- Where FMOps holds project records, they are held in the EU with encryption in transit and at rest, and access limited to server code and the FMOps account.

Organisational measures

- Written record of what is connected, at what scope, and how to disconnect it.
- Breach handling procedure with the 48-hour notification duty in clause 7.
- Annual review of these measures, and after any breach or significant change to the Services.
- Confidentiality duties under clause 5.2 and the Services Agreement.

Resilience

- Backup and restore of the Controller's data remain the responsibility of the Controller's own providers, under the terms the Controller has with them. FMOps does not hold the master copy of the Controller's data, so FMOps is not a point of failure for it.
- Configuration and workflow definitions built for the Controller are documented so they can be rebuilt if a platform fails.

Annex 3 — Sub-processors

Sub-processors FMOps uses that may process the Controller's personal data. Each is engaged under a written contract with data protection terms equivalent to this agreement.

SUB-PROCESSOR	PURPOSE	PROCESSING LOCATION	TRANSFER MECHANISM
Google Ireland Ltd (Workspace)	FMOps email, calendar and documents used to correspond about the engagement	EU, with support access outside the EEA	EU–US Data Privacy Framework and Standard Contractual Clauses

Vercel Inc.	Hosting of fmops.ie, serverless functions and request logs	EU region, United States for company operations	EU–US Data Privacy Framework and Standard Contractual Clauses
Supabase Inc.	Database for enquiries, tool submissions and project records	EU (Ireland) region	Standard Contractual Clauses for company support access
Resend Inc.	Sending transactional email such as confirmations and reports	United States	Standard Contractual Clauses
Calendly LLC	Booking calls, where the Controller's staff book through the FMOps calendar	United States	Standard Contractual Clauses
Anthropic PBC	Only where FMOps sends content to Claude on the Controller's instruction, for example to summarise a report	United States and EU	Anthropic Data Processing Addendum with Standard Contractual Clauses

Where the Controller holds its own contract with a provider — Anthropic for Claude licences, Google or Microsoft for the Controller's email suite, an accounts package, or an automation platform the Controller pays for — that provider is the Controller's processor, not a sub-processor of FMOps, and the Controller's own terms with it apply.

Under Anthropic's commercial terms, which govern Claude for Work, Team and Enterprise plans and the API, Anthropic does not use customer content to train its models.

Additions or replacements are notified under clause 5.4.

FMOps · Fionn Murphy · Waterford, Ireland · fionn@fmops.ie · +353 86 107 2373 · fmops.ie