

Data Processing Addendum

Trilot LLC ("Processor") and **[Client Name] ("Controller")** enter into this Data Processing Addendum ("DPA") in connection with the Engagement Letter dated [date] between the parties (the "Engagement Letter").

This DPA forms part of the Engagement Letter. In case of conflict between this DPA and the Engagement Letter on a data-protection matter, this DPA controls.

1. Definitions

Capitalized terms not defined here have the meanings given in the GDPR, UK GDPR, or applicable equivalent data-protection law.

- "Applicable Data Protection Law" means the GDPR, UK GDPR, EU member-state implementing laws, the Swiss Federal Act on Data Protection, and any other data-protection law applicable to the processing under this DPA.
 - "Client Personal Data" means personal data that the Controller (or the Controller's data subjects) provides to Trilot, or that Trilot accesses or processes, in performing Services under the Engagement Letter.
 - "Sub-processor" means any third party engaged by Trilot to process Client Personal Data on the Controller's behalf.
-

2. Roles

The Controller appoints Trilot as a Processor to process Client Personal Data for the purposes set out in Annex A, on the terms of this DPA.

Trilot acts as Processor only — it does not determine the purposes or essential means of processing Client Personal Data. Where Trilot processes personal data for its own purposes (for example, its own newsletter subscribers), it does so as a Controller and the Trilot Privacy Policy applies, not this DPA.



3. Trilot's obligations

Trilot will:

- (a) Process Client Personal Data only on the Controller's documented instructions, including with regard to international transfers. The Engagement Letter constitutes the initial documented instructions. Additional instructions must be agreed in writing.
- (b) Inform the Controller if, in Trilot's opinion, an instruction from the Controller violates Applicable Data Protection Law.
- (c) Ensure that personnel authorized to process Client Personal Data are bound by confidentiality obligations.
- (d) Implement appropriate technical and organizational measures to protect Client Personal Data, as described in Annex C.
- (e) Engage Sub-processors only on the terms of clause 5 below.
- (f) Assist the Controller, taking into account the nature of the processing and the information available to Trilot, in complying with the Controller's obligations under Articles 32–36 of the GDPR (security, notification of breaches, data-protection impact assessments, and prior consultation).
- (g) Assist the Controller, by appropriate technical and organizational measures, in fulfilling its obligation to respond to data subjects' rights requests under GDPR Chapter III.
- (h) Notify the Controller without undue delay (and in any event within 72 hours) of becoming aware of a personal-data breach affecting Client Personal Data.
- (i) Upon termination of the Engagement Letter, at the Controller's election, delete or return all Client Personal Data, and delete existing copies unless Applicable Data Protection Law requires storage.
- (j) Make available to the Controller all information necessary to demonstrate compliance with this DPA, and allow for audits, including inspections, conducted by the Controller or an auditor mandated by the Controller, on reasonable prior notice, no more than once per twelve-month period, and subject to confidentiality obligations.

4. Controller's obligations

The Controller:

- (a) Warrants that it has all rights, consents, and lawful bases necessary to permit Trilot to process Client Personal Data under this DPA, and that its instructions are lawful.
 - (b) Is responsible for the accuracy, quality, and legality of Client Personal Data and the means by which the Controller acquired it.
 - (c) Will provide Trilot with all information reasonably needed to perform Services in compliance with this DPA and Applicable Data Protection Law.
-

5. Sub-processors

The Controller authorizes Trilot to engage the Sub-processors listed in Annex D for the processing of Client Personal Data.

Trilot will notify the Controller of any intended addition or replacement of a Sub-processor, giving the Controller a reasonable opportunity (not less than fourteen days) to object on reasonable data-protection grounds. If the Controller objects, the parties will discuss in good faith. If no resolution is reached within thirty days, the Controller may terminate the affected engagement without further liability.

Trilot remains liable for the acts and omissions of its Sub-processors with respect to Client Personal Data as if they were Trilot's own.

6. International transfers

Where the processing of Client Personal Data under this DPA involves transfers of personal data from the EEA, the UK, or Switzerland to a country not recognized as providing adequate protection:

- (a) The parties enter into the Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914 of 4 June 2021) as Controller-to-Processor (Module 2) or Processor-to-Processor (Module 3) as applicable, which are incorporated by reference into this DPA. Optional clauses are not included unless expressly agreed in writing.



(b) For transfers subject to UK GDPR, the parties enter into the UK International Data Transfer Addendum to the EU Standard Contractual Clauses (issued by the UK Information Commissioner's Office on 21 March 2022), also incorporated by reference.

(c) For transfers subject to Swiss data-protection law, the SCCs apply with Switzerland-specific modifications recognized by the Swiss Federal Data Protection and Information Commissioner.

(d) Where a Sub-processor is certified under the EU-US Data Privacy Framework (and any applicable UK or Swiss extensions), the relevant DPF certification serves as the transfer safeguard for transfers to that Sub-processor, supplementing or replacing the SCCs at the Controller's discretion.

7. Liability

The liability of each party under this DPA is subject to the limitations and exclusions set out in the Engagement Letter and the Trilot Terms of Service, except where those limits would result in a violation of Applicable Data Protection Law (in which case the maximum amount permitted by such law applies).

8. Term

This DPA takes effect on the Effective Date of the Engagement Letter and continues for as long as Trilot processes Client Personal Data under the Engagement Letter. Clauses that by their nature should survive termination (including audit rights, confidentiality, and the obligation to delete or return Client Personal Data) survive termination.

9. Order of precedence

In the event of any conflict, the order of precedence is: (a) the SCCs and any other transfer mechanisms required by Applicable Data Protection Law; (b) this DPA; (c) the Engagement Letter; (d) the Trilot Terms of Service.

Annex A — Details of processing

Subject matter. Provision of Services under the Engagement Letter.



Duration. For the term of the Engagement Letter and any post-termination period during which Trilot retains Client Personal Data (typically not exceeding 30 days post-termination, except where required by law).

Nature and purpose of processing. As set out in the Engagement Letter. Common examples include: hosting and operating systems that hold the Controller's end-user data; building software that processes end-user personal data; technical audits that involve reading systems containing personal data.

Type of personal data. As specified per engagement. To be filled in for each engagement.

Categories of data subjects. As specified per engagement. Commonly: the Controller's customers, employees, contractors, or other end users of the Controller's systems.

Annex B — Special category data and criminal-conviction data

Trilot does not, by default, process special-category personal data (Article 9 GDPR — racial or ethnic origin, political opinions, religious beliefs, trade-union membership, genetic data, biometric data for unique identification, health data, sex life or sexual orientation data) or criminal-conviction data.

If a specific engagement requires processing of such data, this must be expressly stated in the Engagement Letter, the additional safeguards must be agreed in writing, and additional terms of this DPA may apply.

Annex C — Technical and organizational measures

Trilot maintains the following technical and organizational measures:

Access control:

- Multi-factor authentication on all Trilot operator accounts that have access to Client Personal Data
- Principle of least privilege: personnel access only the data necessary for their tasks
- Quarterly access review

Encryption:



- TLS 1.2+ for all data in transit
- Encryption at rest for systems holding Client Personal Data, where the underlying provider supports it (Cloudflare R2, GitHub, Google Workspace, etc.)

Logical access:

- SSO where supported
- Hardware-token MFA for high-privilege accounts (Cloudflare, GitHub, AWS where applicable)
- Password manager use mandatory for all service accounts

Physical security:

- Trilot operates primarily from secured offices in Amman, Jordan and remote work locations. Cloud-hosted infrastructure is the primary processing environment.

Backup and recovery:

- Regular backups of code and configuration
- Tested restoration procedures
- Backups encrypted at rest

Incident response:

- Documented incident response plan
- 72-hour notification commitment under clause 3(h)

Sub-processor management:

- Each Sub-processor under contract with appropriate data-protection terms
- Annual review of Sub-processor compliance

Personnel:

- Background-checked where the role and jurisdiction permit
- Trained on data-protection obligations annually
- Confidentiality agreements signed before access is granted



Annex D — Approved Sub-processors

SUB - PROCESSOR	ROLE	LOCATION	TRANSFER SAFEGUARD
Cloudflare, Inc.	Hosting, CDN, DNS, security	US, global edge	DPF + SCCs
GitHub, Inc. (Microsoft)	Source-code hosting	US	DPF + SCCs
Google LLC (Workspace)	Email and productivity	US	DPF + SCCs
Resend, Inc.	Transactional email	US	DPF + SCCs
MailerLite (UAB Mailerlite)	Newsletter sending	EU / US	SCCs
Cal.com, Inc.	Calendar booking	US	DPF + SCCs
AWS (via Resend / select integrations)	Underlying infrastructure for some Sub-processors	US, global	DPF + SCCs

(Additional Sub-processors may be engaged as needed and notified to the Controller per clause 5.)

