# ClearPolicy International Data Transfer Agreement

UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses
(Module Two: Controller to Processor)

Version date: 7 July 2026

This agreement supplements the ClearPolicy Data Processing Agreement available at https://www.clearpolicy.app/data-processing-agreement/ and the ClearPolicy Terms of Service. It provides appropriate safeguards for restricted transfers of personal data from the United Kingdom to the United States in connection with use of the ClearPolicy service.

The Data Importer has pre-executed this agreement below. The Customer (Data Exporter) may complete the exporter details in Table 1 and the exporter signature block for their own compliance records. No countersignature from ClearPolicy is required for the agreement to apply to a Customer that has accepted the ClearPolicy Data Processing Agreement.

## Part 1: Tables

### Table 1: Parties

Start date: The date the Customer creates or continues using a ClearPolicy account.

**Data Exporter (Customer)**

Full legal name: _____

Trading name (if different): _____

Main address: _____

Official registration number (if any): _____

Key contact: _____

**Data Importer (ClearPolicy)**

Full legal name: Laconic Company LLC

Trading name (if different): ClearPolicy

Main address: 2120 S Reserve Street PMB 1087, Missoula, MT 59801, United States

Official registration number (if any): N/A

Key contact: Roy McKenzie, support@clearpolicy.app

**Table 2: Selected SCCs, Modules and Selected Clauses**

- Approved EU SCCs: Commission Implementing Decision (EU) 2021/914 of 4 June 2021
- Module Two (Controller to Processor) is in operation
- Clause 7 (Docking Clause): Not used
- Clause 11 (Option): Option 2 — data importer shall not be liable for damages caused by the data exporter or another processor
- Clause 9(a) (Sub-processors): General written authorisation
- Clause 9(a) time period for prior notice of sub-processor changes: 30 days
- Personal data received from the Importer is not combined with personal data collected by the Exporter

**Table 3: Appendix Information**

The Appendix Information is set out in Annexes I.A, I.B, II, and III below.

**Table 4: Ending this Addendum when the Approved Addendum Changes**

Neither Party may end this Addendum under Section 19 when the Approved Addendum changes.

## Part 2: Mandatory Clauses

**Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.**

## Standard Contractual Clauses

The Standard Contractual Clauses set out in the Annex to Commission Implementing Decision (EU) 2021/914 of 4 June 2021, Module Two (Controller to Processor), are incorporated into this agreement and amended as set out in Part 2 of the UK International Data Transfer Addendum above.

## Annex I.A: List of Parties

**Data exporter(s):**

The Customer organization using ClearPolicy, as identified in Table 1

Contact person's name, position and contact details: As identified in Table 1

Activities relevant to the data transferred under these Clauses: Use of the ClearPolicy service

Signature and date: See signature block below

Role: Controller

**Data importer(s):**

Laconic Company LLC (trading as ClearPolicy)

Contact person's name, position and contact details: Roy McKenzie, support@clearpolicy.app

Activities relevant to the data transferred under these Clauses: Provision of the ClearPolicy software-as-a-service platform

Signature and date: See signature block below

Role: Processor

## Annex I.B: Description of Transfer

**Categories of data subjects whose personal data is transferred**

- People added or imported by the Customer (employees, volunteers, contractors, and other recipients)
- Team members who sign in and work inside the Customer's ClearPolicy organization
- Individuals whose data is synced through integrations enabled by the Customer (for example, Planning Center)

**Categories of personal data transferred**

- People records: name, email address, phone number (if provided), group membership, and document request status
- Team member records: name, email address, organization name, role, account preferences, and authentication data
- Signature and acknowledgment records: typed name, timestamp, IP address, browser or user agent, document version, activity history, document integrity hash, and related audit data
- Document content: policies, forms, uploaded PDFs, editor content, exported files, and related metadata
- Communications content: message text included with document requests or in-app product support, where provided by the Customer
- Integration data (if enabled): encrypted authentication tokens, provider account identifiers, and data imported from connected services

**Sensitive data transferred (if applicable) and applied restrictions or safeguards**

The transferred personal data may include special category data or data relating to criminal convictions and offences only where the Customer chooses to include such information in documents, forms, or people records uploaded to ClearPolicy. ClearPolicy does not require such

data and processes it solely on the Customer's instructions. Additional safeguards include access controls, encryption in transit, private object storage, organization data isolation, and role-based access within the product.

**Frequency of the transfer**

Continuous, for the duration of the Customer's use of ClearPolicy.

**Nature of the processing**

- Storing and displaying documents and document revisions
- Sending document requests, reminders, and service-related notifications
- Recording acknowledgments, electronic signatures, timestamps, audit trails, and compliance reports
- Generating exports, receipts, and printable reports
- Operating optional integrations authorized by the Customer
- Securing the service, providing support, and maintaining reliability

**Purpose(s) of the data transfer and further processing**

To provide the ClearPolicy service, including policy and document management, acknowledgment and signature collection, compliance tracking, notifications, exports, and related account administration, as described in the ClearPolicy Data Processing Agreement.

**Period for which the personal data will be retained**

For the term of the Customer's subscription or trial, and as otherwise described in the ClearPolicy Data Processing Agreement (Sections 10 and 11 on data retention and deletion). Completed signature and acknowledgment records may be retained longer to preserve legal and compliance audit trails.

**Transfer to sub-processors and subject matter, nature and duration of processing**

As described in Annex III. The data importer may engage sub-processors to support hosting, storage, email delivery, billing, monitoring, analytics, and optional integrations, subject to the terms of the Standard Contractual Clauses and the ClearPolicy Data Processing Agreement.

## Annex II: Technical and Organisational Measures

The data importer implements administrative, technical, and organisational measures designed to protect personal data, including:

- Hosting production systems on dedicated cloud infrastructure in the United States (Vultr, New Jersey)
- HTTPS/TLS encryption for data in transit

- Private object storage for uploaded documents and files (Cloudflare)
- Encryption at rest for sensitive integration and authentication tokens
- Role-based access controls within the product and organization data isolation
- Team member authentication with optional two-factor authentication
- Access to production systems limited to authorized personnel
- Application monitoring and error tracking to detect and respond to issues

Vultr's New Jersey data center maintains third-party attestations including SOC 1 Type II, SOC 2 Type II, ISO 27001, PCI DSS, and HITRUST. These are infrastructure-provider certifications and do not represent a separate certification held by ClearPolicy itself.

## Annex III: List of Sub-processors

**Core sub-processors (used for all customers):**

- Vultr — application and database hosting (United States, New Jersey)
- Cloudflare — private object storage for uploaded documents and files
- Resend — transactional email delivery (United States)
- Stripe — billing and subscription management for account holders (United States)
- Laravel Nightwatch — application monitoring and error tracking (United States)
- Matomo — product usage analytics (Seattle, United States)
- OpenAI — limited AI-assisted features, including internal organization classification and in-app product support for team members; routine product workflows do not send people records or document content; team members should not include people data or document content in support messages

**Conditional sub-processors (only when the Customer enables the relevant feature):**

- Google — optional Google sign-in and Google Drive document import
- Microsoft — optional Microsoft sign-in
- Planning Center — optional people and list synchronization
- Zapier and authorized API clients — data accessed through integrations and automations configured by the Customer

The current sub-processor list is also published at https://www.clearpolicy.app/data-processing-agreement/. The data importer will provide 30 days' notice of material changes to core sub-processors.

## Signatures

The Data Importer has executed this agreement as set out below. The Customer may complete the exporter signature block for its compliance records.

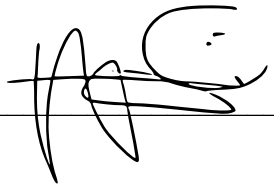
This International Data Transfer Agreement incorporates the UK International Data Transfer Addendum and the EU Standard Contractual Clauses (Module Two), as amended by the UK Addendum.

**Data Importer (Laconic Company LLC / ClearPolicy)**

Name: Roy McKenzie

Title: Owner

Date: 7 July 2026

Signature: 

**Data Exporter (Customer) — optional, for Customer records**

Name: _____

Title: _____

Date: _____

Signature: _____