DATA PROCESSING AGREEMENT

Public version

Version 2.1

This Data Processing Agreement (the **"DPA"**) is entered into between **G2-F Technologies S.L.** (the **"Processor"**), with NIF B24903833, having its registered office at Calle Tirso de Molina 11, 28912, Leganés, Madrid, Spain, and the customer that uses the Services (the **"Controller"**). It forms an integral part of, and is incorporated by reference into, the agreement under which the Processor provides the Services to the Controller (the **"Principal Agreement"**), including the Processor's Terms of Service. By accepting the Principal Agreement, the Controller agrees to this DPA.

Where the Controller requires a countersigned copy reflecting its own details, the Processor will make an executable version available on request.

WHEREAS:

(a) The Processor provides workflow automation and AI-powered document processing services to the Controller under the Principal Agreement;

(b) The Processor will process Personal Data on behalf of the Controller in connection with those services, including through the use of artificial intelligence systems and general-purpose AI models;

(c) The Parties wish to ensure compliance with the General Data Protection Regulation (EU) 2016/679 (**"GDPR"**), Regulation (EU) 2024/1689 on Artificial Intelligence (**"AI Act"**), and all other applicable data protection laws;

(d) This Agreement sets out the rights and obligations of the Parties in relation to the processing of Personal Data and establishes the safeguards required under Article 28 of the GDPR.

THE PARTIES AGREE AS FOLLOWS:

1. Definitions

For the purposes of this Agreement, the following definitions shall apply. Terms not defined herein shall have the meaning given to them in the GDPR or, for AI-related terms, in Regulation (EU) 2024/1689 (the **"AI Act"**).

1.1. **"AI Provider"** means a natural or legal person that develops, operates, or makes available an AI System or a General-Purpose AI Model used by the Processor in the provision of the Services.

1.2. **"AI System"** has the meaning given in Article 3(1) of the AI Act.

1.3. **"AI Output"** means any content, prediction, recommendation, decision, extraction, classification, or other result generated by an AI System in connection with the Services.

1.4. **"Applicable Data Protection Law"** means all laws and regulations applicable to the processing of Personal Data, including the GDPR, the LOPD-GDD, the AI Act, and any national implementing legislation, as amended from time to time.

1.5. **"Customer Data"** means all data, including Personal Data, that the Controller submits, uploads, or otherwise makes available to the Processor in connection with the Services.

1.6. **"LOPD-GDD"** means Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

1.7. **"Platform"** means the Processor's software platform through which the Services are delivered, including all associated APIs, web interfaces, and infrastructure components.

1.8. **"Principal Agreement"** means the master services agreement, order form, or other agreement between the Parties under which the Services are provided.

1.9. **"Services"** means the workflow automation, document processing, data extraction, and related services provided by the Processor to the Controller under the Principal Agreement.

1.10. **"Standard Contractual Clauses"** or **"SCCs"** means the standard contractual clauses for the transfer of personal data to third countries as set out in Commission Implementing Decision (EU) 2021/914, as amended or replaced from time to time.

1.11. **"Sub-processor"** means any processor engaged by the Processor to carry out specific processing activities on behalf of the Controller, including AI Providers that process Personal Data.

2. Scope and Purpose of Processing

2.1. This Agreement applies to the processing of Personal Data by the Processor on behalf of the Controller in connection with the provision of the Services under the Principal Agreement. In the event of any conflict between this Agreement and any other agreement between the Parties, the following order of precedence shall apply: (a) the Standard Contractual Clauses (where applicable); (b) this Agreement; (c) the Principal Agreement.

2.2. The details of the processing operations are set out in Annex A. The Processor shall process Personal Data only for the specific purposes set out in Annex A, unless the Controller provides prior written instructions or processing is required by Applicable Data Protection Law.

2.3. The Processor shall not: (a) process Personal Data for its own purposes; (b) sell, share, or disclose Personal Data

to any third party except as permitted under this Agreement; (c) use Personal Data to train, retrain, or improve any AI model or algorithm, whether directly or through any Sub-processor; or (d) combine Personal Data from the Controller with data from any other source, except as necessary to provide the Services.

3. Controller Obligations

The Controller warrants and undertakes that:

3.1. It has complied and will continue to comply with all Applicable Data Protection Law in respect of its processing of Personal Data and any processing instructions it issues to the Processor.

3.2. It has obtained all necessary consents, authorizations, and legal bases required under Applicable Data Protection Law to enable the lawful transfer of Personal Data to the Processor, including any processing through AI Systems.

3.3. It has provided adequate notice to Data Subjects regarding the processing of their Personal Data, including all disclosures required under Articles 13 and 14 of the GDPR and, where applicable, information about the use of AI Systems.

3.4. All processing instructions given to the Processor shall comply with Applicable Data Protection Law.

3.5. It shall promptly inform the Processor if any Personal Data submitted to the Platform contains Special Categories of Personal Data.

4. Processor Obligations

The Processor warrants and undertakes that:

4.1. It shall process Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data to a Third Country, unless required to do so by Applicable Data Protection Law; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

4.2. It shall immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other Applicable Data Protection Law.

4.3. It shall ensure that persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.4. It shall take all measures required pursuant to Article 32 of the GDPR, as further detailed in Article 8 and Annex B.

4.5. It shall comply with the conditions for engaging Sub-processors as set out in Article 6.

4.6. It shall assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to the Processor.

4.7. At the choice of the Controller, it shall delete or return all Personal Data after the end of the provision of Services and delete existing copies unless Applicable Data Protection Law requires storage of the Personal Data.

4.8. It shall make available to the Controller all information necessary to demonstrate compliance with Article 28 of the GDPR and allow for and contribute to audits conducted by the Controller or another auditor mandated by the Controller.

4.9. It shall maintain records of processing activities carried out on behalf of the Controller in accordance with Article 30(2) of the GDPR.

4.10. Where required by Applicable Data Protection Law, the Processor shall appoint a Data Protection Officer and provide the Controller with the relevant contact details.

5. Artificial Intelligence and Automated Processing

5.1. AI Processing Principles

5.1. Where the Processor uses AI Systems or General-Purpose AI Models in the provision of the Services, the following provisions shall apply in addition to all other obligations under this Agreement.

5.2. The Processor shall process Personal Data through AI Systems only to the extent necessary for the performance of the Services as described in Annex A and shall apply the principles of data minimization and purpose limitation to all AI-related processing.

5.3. The Processor shall not, and shall ensure that its Sub-processors and AI Providers do not, use the Controller's Personal Data to train, retrain, fine-tune, or otherwise improve any AI model. The Processor shall maintain contractual agreements with all AI Providers that expressly prohibit the use of Customer Data for model training. Upon request, the Processor shall provide evidence of such contractual protections.

5.2. AI Output and Transparency

5.1. All AI Output generated from the Controller's Personal Data shall be treated as Personal Data to the extent it contains or can be linked to Personal Data. The Processor shall not retain AI Output longer than necessary for the provision of the Services.

5.2. The Controller acknowledges that AI Output may contain inaccuracies and is responsible for reviewing and validating AI Output before relying upon it.

5.3. The Processor shall, upon request, make available documentation describing the AI Systems used, the categories of Personal Data submitted, and the data retention practices of each AI Provider. Any change to AI Providers shall be subject to the Sub-processor procedures in Article 6.

6. Sub-processors

6.1. The Controller provides general authorization for the Processor to engage Sub-processors, including AI Providers, to process Personal Data on behalf of the Controller, subject to the requirements set out in this Article. The list of authorized Sub-processors as of the Effective Date is set out in Annex C.

6.2. The Processor shall notify the Controller in writing at least 30 days before engaging any new Sub-processor or replacing an existing Sub-processor, providing the name, location, processing activities, and applicable transfer mechanism.

6.3. The Controller may object to the engagement of a new Sub-processor on reasonable grounds relating to data protection within 15 days of receiving the notification. The Parties shall discuss the objection in good faith. If unresolved within 30 days, the Controller may terminate the affected Services without penalty.

6.4. The Processor shall ensure that each Sub-processor is bound by written contractual obligations that provide at least the same level of data protection as this Agreement, meet the requirements of Article 28(3) of the GDPR, and prohibit the use of Personal Data for AI model training or improvement.

6.5. The Processor shall remain fully liable to the Controller for the acts and omissions of its Sub-processors.

6.6. Upon request, the Processor shall provide the Controller with copies of its agreements with Sub-processors (which may be redacted to protect confidential commercial information) and evidence of no-training commitments from AI Providers.

7. Data Subject Rights

7.1. The Processor shall, taking into account the nature of the processing, assist the Controller by appropriate technical and organizational measures for the fulfillment of the Controller's obligation to respond to Data Subject requests under Chapter III of the GDPR (including rights of access, rectification, erasure, restriction, portability, objection, and rights related to automated decision-making).

7.2. If the Processor receives a request from a Data Subject, the Processor shall promptly, and in any event within 5 business days, notify the Controller and shall not respond directly unless authorized by the Controller or required by Applicable Data Protection Law.

7.3. The Processor shall provide reasonable assistance to the Controller in responding to Data Subject requests at no additional charge, unless such requests require significant additional resources beyond what is reasonably anticipated.

8. Security Measures

8.1. The Processor shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 of the GDPR, including the pseudonymization and encryption of Personal Data, the ability to ensure ongoing confidentiality, integrity, availability, and resilience of processing systems, the ability to restore availability in the event of an incident, and a process for regularly testing the effectiveness of such measures.

8.2. The specific security measures implemented by the Processor are described in Annex B (Technical and Organizational Security Measures).

8.3. The Processor shall ensure that any person acting under its authority who has access to Personal Data is subject to a duty of confidentiality and processes Personal Data only on instructions from the Controller.

8.4. The Processor shall not materially reduce the overall level of security provided under this Agreement during its term without the Controller's prior written consent.

9. Personal Data Breach

9.1. Notification Requirements

9.1. The Processor shall notify the Controller without undue delay, and in any event within 48 hours, after becoming aware of a Personal Data Breach affecting Personal Data processed on behalf of the Controller.

9.2. The notification shall include: (a) the nature of the breach, including where possible the categories and approximate number of Data Subjects and records concerned; (b) the contact details of the Processor's data protection officer or point of contact; (c) the likely consequences of the breach; and (d) the measures taken or proposed to address the breach and mitigate its effects.

9.3. Where it is not possible to provide all information at the same time, the Processor shall provide information in phases without undue further delay.

9.2. Cooperation

9.1. The Processor shall cooperate with the Controller to investigate the breach, identify affected Data Subjects, assess the risk, prepare any required notifications, and implement measures to mitigate the effects and prevent recurrence.

9.2. The Processor shall not communicate any Personal Data Breach to Data Subjects, Supervisory Authorities, or the media without the prior written consent of the Controller, unless required by Applicable Data Protection Law.

9.3. The Processor shall document all Personal Data Breaches, including facts, effects, and remedial action taken, and make such documentation available to the Controller upon request.

10. International Data Transfers

10.1. General Principle

10.1. The Processor shall process Personal Data within the European Economic Area (EEA). The Processor shall not transfer Personal Data to a Third Country unless the Controller has provided prior written authorization (which is deemed granted for the transfers described in Annex C) and appropriate safeguards are in place in accordance with Chapter V of the GDPR.

10.2. Authorized Transfer Mechanisms

10.1. Transfers to Third Countries may be made where one of the following conditions is met:

10.1.1. An adequacy decision by the European Commission pursuant to Article 45 of the GDPR;

10.1.2. Standard Contractual Clauses approved by the European Commission pursuant to Article 46(2)(c) of the GDPR;

10.1.3. Binding Corporate Rules approved pursuant to Article 47 of the GDPR;

10.1.4. The EU-US Data Privacy Framework, where the recipient is a certified participant.

10.2. Where Standard Contractual Clauses are used, the Processor shall complete a transfer impact assessment and implement supplementary measures where necessary to ensure an essentially equivalent level of protection.

10.3. Government Access Requests

10.1. The Processor shall notify the Controller promptly if it receives a request from a government authority for access to Personal Data, unless prohibited by law. The Processor shall not disclose Personal Data to any government authority unless legally compelled to do so, and shall in such case disclose only the minimum amount necessary and notify the Controller as soon as legally permitted.

11. Audit Rights

11.1. Right to Audit

11.1. The Processor shall make available to the Controller all information necessary to demonstrate compliance with Article 28 of the GDPR and shall allow for and contribute to audits, including inspections, conducted by the Controller or an independent auditor mandated by the Controller.

11.2. The Controller shall provide the Processor with at least 30 days' prior written notice of any audit, unless a shorter period is required by a Supervisory Authority or a Personal Data Breach has occurred. Audits shall be conducted during normal business hours and shall not unreasonably disrupt the Processor's operations.

11.3. Each Party shall bear its own costs associated with audits. If an audit reveals material non-compliance by the Processor, the Processor shall bear the reasonable costs of the audit. The Controller shall not conduct more than one audit per calendar year, unless required due to a breach or evidence of non-compliance.

11.2. Certifications and Reports

11.1. The Processor may satisfy audit requirements, in whole or in part, by providing current certifications (such as ISO 27001 or SOC 2 Type II), summary audit reports from independent third parties, or responses to industry-standard security questionnaires.

11.2. The Controller retains the right to conduct its own audit notwithstanding any certifications or reports provided, where the Controller has reasonable grounds to believe that such certifications are insufficient or a Personal Data Breach has occurred.

11.3. All information obtained during an audit shall be treated as confidential and shall only be used for the purpose of verifying compliance with this Agreement.

12. Term and Termination

12.1. Term

12.1. This Agreement shall commence on the Effective Date and shall remain in force for the duration of the Principal Agreement. Upon termination or expiration of the Principal Agreement, this Agreement shall automatically terminate, subject to the survival provisions set out in this Article.

12.2. Termination for Breach

12.1. Either Party may terminate this Agreement immediately upon written notice if the other Party commits a material breach that is not remedied within 30 days of receiving written notice specifying the breach.

12.2. The Controller may terminate this Agreement immediately upon written notice if the Processor processes Personal Data in a manner that constitutes a material breach of Applicable Data Protection Law or fails to comply with a final and binding decision of a Supervisory Authority.

12.3. Return or Deletion of Personal Data

12.1. Upon termination of this Agreement, and at the choice of the Controller, the Processor shall return all Personal Data in a structured, commonly used, and machine-readable format and/or delete all Personal Data, including all copies and data held by Sub-processors.

12.2. The Controller shall notify the Processor of its choice within 30 days of termination. If no notification is received, the Processor shall delete all Personal Data. The Processor shall complete the return or deletion within 30 days and

provide written certification of completion.

12.3. The Processor may retain Personal Data after termination only where required by Applicable Data Protection Law or necessary for the establishment, exercise, or defense of legal claims. Any retained data shall be isolated, protected, and deleted as soon as the legal basis for retention no longer applies.

12.4. Survival

12.1. The following provisions shall survive termination: confidentiality obligations (Article 14), liability provisions (Article 13), data return and deletion obligations (this Article 12), and audit rights with respect to the period prior to termination (Article 11).

13. Liability and Indemnification

13.1. Allocation of Liability

13.1. Each Party shall be liable for damages caused by processing that infringes this Agreement or Applicable Data Protection Law, in accordance with Article 82 of the GDPR.

13.2. The Processor shall be liable for damages caused by processing only where it has not complied with obligations of the GDPR specifically directed to Processors or where it has acted outside or contrary to the lawful instructions of the Controller.

13.3. The Processor shall be liable for the acts and omissions of its Sub-processors to the same extent as if such acts and omissions were performed by the Processor itself.

13.2. Indemnification

13.1. The Processor shall indemnify the Controller against all claims, losses, damages, and reasonable legal fees arising from any breach by the Processor of its obligations under this Agreement or any processing not in accordance with the Controller's documented instructions.

13.2. The Controller shall indemnify the Processor against all claims, losses, damages, and reasonable legal fees arising from any breach by the Controller of its obligations under this Agreement or any processing instructions that infringe Applicable Data Protection Law.

13.3. Limitation of Liability

13.1. The liability of each Party under this Agreement shall be subject to the limitations of liability set out in the Principal Agreement.

13.2. Nothing in this Agreement shall exclude or limit either Party's liability for fraud, fraudulent misrepresentation, or any liability that cannot be excluded by Applicable Data Protection Law.

14. General Provisions

14.1. Confidentiality

14.1. Each Party shall keep confidential all Personal Data and any information relating to the other Party's business, operations, and security measures obtained in connection with this Agreement. This obligation shall survive the termination of this Agreement.

14.2. The duty of confidentiality shall not apply to information that is publicly available, was lawfully in the receiving Party's possession prior to disclosure, is obtained from a third party without restriction, or is required to be disclosed by law or regulatory authority.

14.2. Amendments

14.1. This Agreement may only be amended by written agreement signed by both Parties. The Processor may update the Annexes to reflect changes in Sub-processors (in accordance with Article 6), enhance security measures, or comply with changes in Applicable Data Protection Law, provided that no amendment shall materially reduce the level of data protection without the Controller's prior written consent.

14.3. Notices

14.1. All notices under this Agreement shall be in writing. Notices relating to Personal Data Breaches shall be sent to: team@g2-f.com.

14.4. Governing Law and Jurisdiction

14.1. This Agreement shall be governed by the laws of Spain. Any disputes shall be submitted to the exclusive jurisdiction of the courts of Madrid.

14.2. Nothing in this Agreement shall limit the rights of Data Subjects or Supervisory Authorities under Applicable Data Protection Law.

14.5. Miscellaneous

14.1. This Agreement, together with the Annexes and the Principal Agreement, constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes all prior agreements relating to data processing arrangements.

14.2. Neither Party may assign this Agreement without the prior written consent of the other Party, except in connection

with a merger, acquisition, or sale of all or substantially all of its assets.

14.3. If any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions shall continue in full force and effect.

14.4. The Processor shall cooperate with and assist the Controller in responding to any inquiries or investigations by a Supervisory Authority relating to the processing of Personal Data under this Agreement.

A. Processing Details

This Annex forms an integral part of the Data Processing Agreement and sets out the details of the processing activities.

A.1 Subject Matter and Purpose of Processing

Subject Matter	Processing of Customer Data in connection with workflow automation, document processing, data extraction, and AI-powered analysis services under the Principal Agreement.
Purpose	(a) Automated extraction of data from documents uploaded by the Controller; (b) AI-powered analysis and classification of documents; (c) workflow automation for the Controller's business processes; (d) secure storage and hosting of Customer Data; (e) generation of reports and outputs as instructed by the Controller.
Duration	For the duration of the Principal Agreement. Upon termination, Article 12 applies.

A.2 Categories of Data Subjects

The Personal Data processed may concern the following categories of Data Subjects, as determined by the Controller's use of the Services:

- Employees, officers, and contractors of the Controller and its clients
- Customers, suppliers, and business partners of the Controller
- Natural persons whose data is contained in documents uploaded to the Platform

A.3 Categories of Personal Data

The following categories of Personal Data may be processed, depending on the documents and data submitted by the Controller:

- **Identification data**: full name, title, position, employee ID, national identification numbers
- **Contact data**: email address, telephone number, postal address
- **Professional data**: employer, job title, professional qualifications, license numbers
- **Financial data**: bank account details, tax identification numbers, invoice data, payment information
- **Technical data**: IP address, device identifiers, Platform usage logs, authentication data
- **Document content**: any Personal Data contained within documents uploaded by the Controller

Note: The Controller determines the categories of Personal Data submitted to the Platform.

A.4 Special Categories of Personal Data

The Services are not designed to process Special Categories of Personal Data. However, Special Categories may be incidentally contained in documents uploaded by the Controller. The Controller is responsible for ensuring a valid legal basis under Article 9 of the GDPR.

A.5 Location of Processing

Primary Location	European Union – AWS eu-central-1 (Frankfurt) and eu-south-2 (Spain)
AI Processing	EEA entities of AI Providers (OpenAI Ireland Ltd., Google Ireland Limited). Where AI processing involves US-based infrastructure (Anthropic PBC), the transfer mechanisms in Annex C apply.

B. Technical and Organizational Security Measures

This Annex forms an integral part of the Data Processing Agreement and describes the technical and organizational security measures implemented by the Processor in accordance with Article 32 of the GDPR.

Measure	**Description**
Access Control	Role-based access control (RBAC); multi-factor authentication (MFA) mandatory for all systems processing Personal Data; unique user identification; privileged access restricted on a need-to-know basis; periodic access reviews and prompt revocation upon role change or termination.
Encryption	AES-256 encryption at rest on all storage systems; TLS 1.2+ encryption in transit for all connections; encrypted database connections and inter-service communications; secure key management with key rotation.
Data Segregation	Logical separation of Customer Data between Controllers at the application and database level; network segmentation between production and non-production environments; separate development, staging, and production environments.
Network Security	Web application firewall (WAF) and DDoS protection via Cloudflare; API endpoints protected by authentication and rate limiting; regular vulnerability scanning; periodic penetration testing.

Measure	Description
Application Security	Secure software development lifecycle (SDLC) with code review; static application security testing (SAST); dependency scanning for known vulnerabilities; input validation and output encoding.
Logging & Monitoring	Centralized logging of security-relevant events; an append-only, tamper-evident audit trail (with a cryptographic per-record hash chain) recording authentication, access-control, credential, and Personal Data access and change events, protected against modification and deletion by database-level controls and write-once (WORM) archival; retention of at least eighteen (18) months in the operational system with long-term archival of aged records; automated integrity verification and alerting for anomalous activity, access denials, and security incidents.
Backup & Recovery	Automated daily backups; encrypted backup storage within the EEA; regular backup restoration testing; documented disaster recovery procedures; RTO and RPO of 24 hours.
Personnel Security	Written confidentiality obligations (NDA) for all employees with access to Personal Data; data protection and security training upon onboarding and periodically thereafter; access revocation upon termination of employment.
Incident Management	Documented incident response plan with defined roles and escalation procedures; 48-hour breach notification commitment; post-incident review and root cause analysis.
Physical Security	Infrastructure hosted on enterprise cloud platforms (AWS) with ISO 27001 and SOC 2 certified data centers; cloud provider facilities secured with 24/7 security, biometric access, and CCTV.
AI Processing Security	AI Provider API access via encrypted and authenticated connections; no retention of Customer Data by AI Providers beyond the API request; input validation to mitigate prompt injection; output filtering; data segregation between Controllers in AI pipelines.
Vendor Security	Due diligence assessment of Sub-processors before engagement; contractual obligations requiring appropriate security measures. Sub-processor certifications: AWS (ISO 27001, SOC 1/2/3), Google Cloud (ISO 27001, SOC 2/3), Microsoft (ISO 27001, SOC 2), Cloudflare (ISO 27001, SOC 2 Type II), Anthropic (SOC 2), Stripe (PCI DSS Level 1, SOC 2), HubSpot (SOC 2 Type II, ISO 27001), PostHog (SOC 2 Type II).

C. Authorized Sub-processors

This Annex forms an integral part of the Data Processing Agreement and lists the Sub-processors authorized by the Controller to process Personal Data.

C.1 Current Sub-processors

The following Sub-processors are authorized to process Personal Data on behalf of the Controller as of the Effective Date:

Sub-processor	Location	Processing Activity	Data Location	Transfer Mechanism
Amazon Web Services EMEA SARL	Luxembourg	Cloud infrastructure, compute, storage, hosting	EU (Frankfurt, Spain)	EEA – no transfer
Google Ireland Limited	Ireland	Cloud infrastructure, AI model inference (Vertex AI, Gemini)	EEA	EEA – no transfer
Microsoft Ireland Operations Limited	Ireland	Cloud infrastructure, productivity services	EEA (EU Data Boundary)	EEA – no transfer
OpenAI Ireland Ltd	Ireland	AI model inference, document extraction, natural language processing	EEA	SCCs (Module 3)
Anthropic PBC	USA (San Francisco)	AI model inference, natural language processing	USA	SCCs (Module 3), UK Addendum
Cloudflare, Inc.	USA (San Francisco)	CDN, DDoS protection, DNS, web application firewall	Global network	EU-US DPF, SCCs
Stripe Payments Europe, Limited	Ireland	Payment processing and billing (acts as independent / joint controller for payment data)	EEA / USA	EU-US DPF, SCCs
HubSpot Ireland Limited	Ireland	CRM, customer communications and marketing	EEA / USA	EU-US DPF, SCCs

Sub-processor	Location	Processing Activity	Data Location	Transfer Mechanism
PostHog, Inc.	USA (San Francisco)	Product analytics and usage telemetry (behavioral events, feature usage)	EEA (Frankfurt)	SCCs

All AI Providers listed above operate under API terms that prohibit the use of Customer Data for model training. Written data processing agreements incorporating Article 28 GDPR obligations are in place with each Sub-processor.

C.2 Updates to This Annex

This Annex will be updated by the Processor in accordance with Article 6 of this Agreement. The Controller will be notified of any additions or changes to the list of Sub-processors at least 30 days in advance.

Last Updated: July 3, 2026

Version: 2.1