DATA PROCESSING ADDENDUM

Version 1.0 · Last updated May 15, 2026

This Data Processing Addendum ("**DPA**") forms part of the CloudOffix Subscription Agreement published at cloudoffix.com/terms, or any other written agreement under which CloudOffix Inc. ("**CloudOffix**") provides the Service to the customer identified in an Order Form ("**Customer**") (the "**Agreement**"). CloudOffix and Customer are each a "**Party**" and together the "**Parties**".

This DPA applies automatically whenever CloudOffix Processes Customer Personal Data under the Agreement, and takes effect on the Agreement's Effective Date. This DPA is published at cloudoffix.com/dpa. No separate signature is needed. Customers that require a countersigned copy may sign the optional signature page at the end of this DPA and send it to legal@cloudoffix.com.

1. Purpose and Scope

1.1 This DPA sets out the Parties' obligations for CloudOffix's Processing of Customer Personal Data in providing the Service, Professional Services and support under the Agreement.

1.2 If this DPA conflicts with the Agreement on the Processing of Personal Data, this DPA prevails to the extent of the conflict. Otherwise the Agreement continues to apply unchanged.

1.3 Capitalized terms not defined in this DPA have the meanings given in the Agreement.

2. Definitions

2.1 "**Applicable Data Protection Laws**" means all laws that apply to the Processing of Customer Personal Data under the Agreement, including, where applicable: (a) Regulation (EU) 2016/679 ("**GDPR**"); (b) the GDPR as it forms part of UK law ("**UK GDPR**") and the UK Data Protection Act 2018; (c) the Swiss Federal Act on Data Protection ("**FADP**"); (d) US State Privacy Laws; and (e) the Turkish Personal Data Protection Law No. 6698 ("**KVKK**").

2.2 "**US State Privacy Laws**" means the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("**CCPA**"), and other US state comprehensive privacy laws, with their regulations.

2.3 "**Customer Personal Data**" means Personal Data contained in Customer Data that CloudOffix Processes on Customer's behalf under the Agreement.

2.4 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data. It does not include unsuccessful attempts that do not compromise the security of Customer Personal Data.

2.5 "**Subprocessor**" means any third party engaged by CloudOffix to Process Customer Personal Data.

2.6 "**Standard Contractual Clauses**" or "**SCCs**" means the standard contractual clauses approved by European Commission Implementing Decision (EU) 2021/914, and "**UK Addendum**" means the International Data Transfer Addendum issued by the UK Information Commissioner.

2.7 "Controller", "Processor", "Data Subject", "Personal Data", "Processing" and "Supervisory Authority" have the meanings given in the GDPR. For US State Privacy Laws, "Controller" includes a "business" and "Processor" includes a "service provider" or "processor" as defined in those laws.

3. Roles and Instructions

3.1 For Customer Personal Data, Customer acts as Controller (or as Processor on behalf of another Controller), and CloudOffix acts as Processor (or as Subprocessor, where Customer is a Processor). Customer determines the purposes and means of the Processing.

3.2 CloudOffix will Process Customer Personal Data only on Customer's documented instructions. The Agreement, this DPA, Customer's configuration and use of the Service, and other reasonable written instructions consistent with the Agreement are Customer's complete instructions.

3.3 CloudOffix will not: (a) sell or share Customer Personal Data; (b) Process it for advertising or marketing purposes of its own; (c) use it to train artificial intelligence models offered to other customers; or (d) Process it for any purpose other than providing, securing, supporting and maintaining the Service, except as required by law.

3.4 If applicable law requires CloudOffix to Process Customer Personal Data other than on Customer's instructions, CloudOffix will inform Customer before Processing, unless the law prohibits such notice.

3.5 CloudOffix will promptly inform Customer if, in its reasonable opinion, an instruction infringes Applicable Data Protection Laws. CloudOffix may suspend Processing under that instruction until Customer confirms or changes it.

4. Customer Responsibilities

4.1 Customer is responsible for: (a) the lawfulness of its Processing of Personal Data and of its instructions to CloudOffix; (b) having a valid legal basis for collecting Customer Personal Data and providing it to CloudOffix; (c) giving Data Subjects all required notices and obtaining all required consents; and (d) configuring and using the Service in line with Applicable Data Protection Laws.

4.2 Customer will not instruct CloudOffix to Process Personal Data in violation of Applicable Data Protection Laws.

5. Details of Processing

5.1 The subject matter, nature, purpose and duration of the Processing, and the categories of Data Subjects and Personal Data, are described in Annex I.

6. Confidentiality and Personnel

6.1 CloudOffix will ensure that personnel authorized to Process Customer Personal Data: (a) are bound by written or statutory confidentiality obligations that survive the end of their engagement; (b) access Customer Personal Data only where needed to perform their duties; and (c) receive appropriate data protection and information security training.

7. Security of Processing

7.1 Taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the Processing, and the risks to Data Subjects, CloudOffix will implement and maintain appropriate technical and organizational measures to protect Customer Personal Data, as described in Annex III.

7.2 Security measures may evolve as technology and threats change, but CloudOffix will not materially decrease the overall security of the Service during a Subscription Term.

8. Personal Data Breach

8.1 CloudOffix will notify Customer without undue delay, and in any case within 72 hours, after confirming a Personal Data Breach.

8.2 To the extent the information is available, the notice will describe: (a) the nature of the Personal Data Breach; (b) the categories and approximate number of Data Subjects and records concerned; (c) its likely consequences; (d) the measures taken or proposed to address it; and (e) a contact point for more information. Where not all information is available at once, CloudOffix may provide it in phases without further undue delay.

8.3 CloudOffix will take reasonable steps to contain, investigate and remediate the Personal Data Breach and to mitigate its effects.

8.4 This Section 8 does not apply to incidents caused by Customer or its Authorized Users. Notification of a Personal Data Breach is not an acknowledgement of fault or liability.

9. Data Subject Rights

9.1 Taking into account the nature of the Processing, CloudOffix will assist Customer by appropriate technical and organizational measures, insofar as possible, in responding to requests from Data Subjects exercising their rights under Applicable Data Protection Laws. The Service allows Customer to access, correct, export and delete Customer Personal Data itself.

9.2 If CloudOffix receives a request directly from a Data Subject, it will, where legally permitted, refer the Data Subject to Customer or notify Customer, and will not respond itself except on Customer's instructions or where required by law.

9.3 Where Customer cannot address a request through the Service, CloudOffix will provide commercially reasonable assistance on request. To the extent legally permitted, Customer will bear the reasonable costs of such additional assistance.

10. Assistance to Customer

10.1 Taking into account the nature of the Processing and the information available to it, CloudOffix will provide reasonable assistance with Customer's obligations relating to security of Processing, Personal Data Breach notifications, data protection impact assessments and prior consultations with Supervisory Authorities, to the extent they relate to CloudOffix's Processing of Customer Personal Data and Customer does not otherwise have access to the relevant information. Assistance beyond the information and documentation CloudOffix makes generally available is at Customer's reasonable cost.

11. Subprocessors

11.1 Customer gives CloudOffix general authorization to engage Subprocessors. The Subprocessors in use at the date of this DPA are listed in Annex II, and Customer consents to them.

11.2 CloudOffix will enter into a written agreement with each Subprocessor imposing data protection obligations no less protective of Customer Personal Data than those in this DPA, and remains responsible for each Subprocessor's performance of those obligations.

11.3 CloudOffix will keep the current list of Subprocessors published at cloudoffix.com/dpa, with a way to subscribe to updates. CloudOffix will publish any addition or replacement of a Subprocessor at least 30 days before it takes effect, and will notify Customers who subscribe by email at the same time.

11.4 Customer may object to a new Subprocessor on reasonable data protection grounds by written notice within 15 days after the change is published; otherwise the change is deemed accepted. The Parties will work in good faith to resolve a timely objection. If they cannot do so within 30 days, Customer may, as its sole remedy, terminate the affected Order Form and receive a refund of prepaid Fees under Section 5.4 of the Agreement.

12. AI Features

12.1 Customer Data used by AI Features remains stored in Customer's CloudOffix database. To generate an output, AI Features send only the content needed for that request to the AI model providers listed in Annex II.

12.2 CloudOffix uses these providers under zero data retention terms: they do not retain Customer Personal Data after processing the request and do not use it to train their models.

12.3 AI Features are used only where Customer enables them, and Customer may disable them at any time.

13. Data Location

13.1 Customer Data is hosted in the region stated in the Order Form. A specific data residency commitment applies only where it is stated in the Order Form or otherwise agreed in writing.

13.2 A hosting commitment does not prevent: (a) remote access needed to provide, secure or support the Service; or (b) Processing by the AI model providers and email delivery provider listed in Annex II in the locations stated there. Any such Processing will comply with this DPA and, where required, a valid transfer mechanism under Section 14.

14. International Data Transfers

14.1 CloudOffix will not transfer Customer Personal Data subject to the GDPR, UK GDPR or FADP to a country without an adequacy decision unless a valid transfer mechanism under Applicable Data Protection Laws applies.

14.2 Where a transfer of Personal Data from the European Economic Area requires it, the SCCs are incorporated into this DPA as follows: (a) Module Two (Controller to Processor) applies where Customer is a Controller; (b) Module Three (Processor to Processor) applies where Customer is a Processor; (c) the optional docking clause in Clause 7 applies; (d) for Clause 9, option 2 (general authorization) applies with the notice period in Section 11.3; (e) for Clauses 17 and 18, the law and courts of Ireland apply; and (f) Annexes I to III of the SCCs are completed with the information in Annexes I to IV of this DPA.

14.3 For transfers from the United Kingdom, the UK Addendum applies, completed with the information in this DPA. For transfers from Switzerland, the SCCs apply with the references to the GDPR read as references to the FADP and the Swiss Federal Data Protection and Information Commissioner as the competent Supervisory Authority.

14.4 For Customer Personal Data subject to the KVKK, transfers abroad will be made under a transfer mechanism permitted by the KVKK, including the standard contract published by the Turkish Personal Data Protection Authority where required.

14.5 Nothing in this DPA modifies the SCCs. If this DPA conflicts with the SCCs, the SCCs prevail.

15. US State Privacy Laws

15.1 For Customer Personal Data subject to US State Privacy Laws, CloudOffix acts as Customer's service provider or processor and will Process it only for the business purposes set out in the Agreement.

15.2 CloudOffix will not: (a) sell or share Customer Personal Data; (b) retain, use or disclose it outside the direct business relationship with Customer or for any purpose other than those business purposes; or (c) combine it with personal information it receives from or on behalf of others, except as US State Privacy Laws permit.

15.3 CloudOffix will comply with applicable US State Privacy Laws, provide the same level of privacy protection they require, and notify Customer if it determines it can no longer meet its obligations

under them. Customer may then take reasonable steps to stop and remediate any unauthorized Processing.

16. Government Requests

16.1 Unless legally prohibited, CloudOffix will promptly notify Customer of any legally binding request by a public authority to access Customer Personal Data.

16.2 CloudOffix will review each request, challenge requests it reasonably considers unlawful, and disclose only the minimum Customer Personal Data it is legally required to disclose.

17. Return and Deletion

17.1 During the Subscription Term, Customer may access, export and delete Customer Data through the Service.

17.2 After expiration or termination of the Agreement, CloudOffix will return and delete Customer Personal Data as set out in Section 5.5 of the Agreement: export on Customer's request made within 30 days, deletion from production systems within 30 days after that period, and deletion from backups within the normal backup rotation of no more than 90 days.

17.3 Customer Personal Data that law requires CloudOffix to retain will remain protected under this DPA and will not be Processed for any other purpose.

18. Audits

18.1 CloudOffix will make available to Customer the information reasonably necessary to demonstrate compliance with this DPA and Article 28 of the GDPR. CloudOffix may meet this obligation with independent audit reports or certifications, security documentation, summaries of penetration tests or vulnerability assessments, and answers to reasonable security and privacy questionnaires.

18.2 Customer may request an audit, by itself or through an independent auditor, only where: (a) the information under Section 18.1 is reasonably insufficient to demonstrate compliance; (b) Customer has received notice of a Personal Data Breach; or (c) an audit is required by Applicable Data Protection Laws or a competent Supervisory Authority.

18.3 Any audit: (a) may take place no more than once in any 12-month period, except under Section 18.2(b) or (c); (b) requires at least 30 days' written notice; (c) will be limited to the Processing of Customer Personal Data, conducted during normal business hours and without unreasonable disruption; (d) will be subject to CloudOffix's reasonable security and confidentiality requirements and give no access to other customers' data; (e) may not be conducted by a competitor of CloudOffix; and (f) will be at Customer's expense. The Parties will agree the scope, timing and duration in advance.

19. Records and Cooperation

19.1 CloudOffix will maintain records of its Processing activities and cooperate with competent Supervisory Authorities as required by Applicable Data Protection Laws.

20. Liability

20.1 Each Party's liability arising out of or relating to this DPA, including the SCCs, is subject to the limitations and exclusions of liability in the Agreement, except to the extent Applicable Data Protection Laws prohibit them.

20.2 Nothing in this DPA limits the rights of Data Subjects or Supervisory Authorities that cannot lawfully be limited by contract.

21. Term and General Provisions

21.1 This DPA remains in force for as long as CloudOffix Processes Customer Personal Data. Provisions that by their nature should survive, including those on confidentiality, deletion, transfers and audits, survive for as long as CloudOffix retains Customer Personal Data.

21.2 Except as required by the SCCs, the governing law and dispute resolution provisions of the Agreement apply to this DPA.

21.3 CloudOffix may update this DPA by publishing a new version at cloudoffix.com/dpa. Updates that do not materially reduce the protection of Customer Personal Data, such as changes required by law or updates to the Subprocessor list under Section 11, apply when published. Any other change applies to an existing Customer only with its written agreement, or from a renewal term that begins at least 30 days after CloudOffix notifies Customer of the change by email.

21.4 If any provision of this DPA is held invalid or unenforceable, the remaining provisions remain in full force and effect. This DPA may be signed electronically and in counterparts.

ANNEX I: DETAILS OF PROCESSING

Subject matter. Processing of Customer Personal Data to provide, operate, maintain, secure and support the Service under the Agreement and Customer's documented instructions.

Duration. For the term of the Agreement, and afterwards until Customer Personal Data is deleted under Section 17.

Nature and purpose. Depending on the applications and features Customer selects and configures, Processing may include collection, recording, organization, structuring, storage, retrieval, consultation, use, transmission, synchronization, integration, modification, analysis, workflow automation, communication, AI-assisted processing where enabled by Customer, support and troubleshooting, backup and recovery, security monitoring and deletion. The purposes are providing the Service, enabling Customer's business processes, providing support, protecting the security and integrity of the Service, and following Customer's documented instructions.

Categories of Data Subjects. Depending on Customer's use of the Service: Customer's employees, Authorized Users, contractors and consultants; job applicants and candidates; customers, prospects, leads and business contacts; suppliers, vendors and partners; event participants and support requesters; Customer's end users; and other individuals whose Personal Data Customer chooses to Process through the Service.

Categories of Personal Data. Depending on Customer's configuration and use of the Service: names and contact details; job title and employer; account and user identifiers; authentication and access information; IP addresses and technical logs; CRM, sales and transaction information; communications and correspondence; meeting and event information; recruitment, CV, education and qualification information; HR and employment information; project, task, workflow and support records; documents, files and attachments; and other Personal Data Customer submits to the Service.

Special categories of Personal Data. The Service does not require special categories of Personal Data. If Customer chooses to Process them, Customer is responsible for ensuring a valid legal basis and any additional safeguards required by Applicable Data Protection Laws.

Frequency. Continuous, or as initiated by Customer and its Authorized Users, throughout the Subscription Term.

ANNEX II: SUBPROCESSORS

The Subprocessors used depend on Customer's hosting region and the features Customer enables.

Subprocessor	Function	Location	Data processed
DigitalOcean, LLC	Primary cloud hosting and virtual infrastructure	United States / EU	Production databases, files and server volumes
Amazon Web Services, Inc.	Encrypted backup storage and secondary infrastructure	United States / EU	Encrypted database backups, DNS records and attachments
ICT Bulut Bilişim A.Ş. (Bulutistan)	Local cloud hosting	Türkiye / Azerbaijan	Production databases, files and server volumes (customers hosted in this region only)
DT Cloud Teknoloji A.Ş.	Local cloud hosting	Türkiye	Production databases, files and server volumes (customers hosted in this region only)
Mailgun Technologies, Inc.	Delivery of emails sent from the Service	United States / EU	Email addresses, message content and delivery logs
OpenAI, L.L.C.	AI model processing for AI Features, under zero data retention	United States	Content of AI requests, not retained after processing
Anthropic, PBC	AI model processing for AI Features, under zero data retention	United States	Content of AI requests, not retained after processing
Google LLC	AI model processing for AI Features, under zero data retention	United States	Content of AI requests, not retained after processing

Third-party applications that Customer connects or buys directly, such as data enrichment providers, are not CloudOffix Subprocessors; their use is governed by Section 2.9 of the Agreement.

ANNEX III: TECHNICAL AND ORGANIZATIONAL MEASURES

Network and infrastructure security. Firewalls, load balancing and isolated Virtual Private Cloud environments. Administrative access is restricted, performed through VPN and SSH key-based authentication, and logged.

Access control. Access to infrastructure and Customer Personal Data is limited to authorized personnel on a need-to-know and least-privilege basis. Database credentials are not exposed to end users.

Customer data isolation. Each customer has a logically separate database. Customers cannot access another customer's database, and database interactions are mediated by the CloudOffix application layer.

Encryption. Customer Data is encrypted in transit using TLS and encrypted at rest in production databases, file storage and backups.

Authentication. Password security controls for users, with two-factor authentication available depending on the environment and configuration. Administrative infrastructure access uses key-based authentication.

Monitoring and logging. Infrastructure, network traffic, system logs and critical parameters are monitored, with alerting designed to detect anomalies, service degradation and security incidents.

Vulnerability and patch management. Processes to identify and remediate vulnerabilities and apply security patches, prioritized by severity.

Backup and recovery. Daily backups and disaster recovery procedures, with backups kept in separate infrastructure where the deployment allows.

Availability and resilience. Infrastructure redundancy, load balancing, failover and scalable server resources.

Secure development and change management. Changes are tested in staging before production, including functional, performance and security validation appropriate to the change.

Incident management. Procedures to detect, investigate, respond to and remediate security incidents. Personal Data Breaches are handled under Section 8.

AI processing. AI requests contain only the content needed for the request and are sent to AI model providers under zero data retention terms, as described in Section 12.

Physical security. CloudOffix relies on established cloud and data center providers that are responsible for the physical security of their facilities.

ANNEX IV: TRANSFER INFORMATION

Data exporter. Customer, as identified in the Order Form, acting as Controller or Processor. Contact: the privacy or notice contact stated in the Order Form.

Data importer. CloudOffix Inc., 6751 Columbia Gateway Drive, Suite 300, Columbia, Maryland 21046, United States, acting as Processor or Subprocessor. Contact: legal@cloudoffix.com.

Description of the transfer. As set out in Annex I. Transfers are continuous for the term of the Agreement.

Technical and organizational measures. As set out in Annex III.

Subprocessors. As listed in Annex II.

Competent Supervisory Authority. The authority determined under Clause 13 of the SCCs.

Signatures

Optional. This DPA applies without signature. Customers that require a countersigned copy may sign below.

CloudOffix Inc.	**Customer:** _____
Signature: _____	Signature: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____