Data processing agreement

This Data Processing Agreement ("**DPA**") governs Alfa Blockchain Consulting's ("**Alfa**") processing of Customer Data (i) provided by Customer to Alfa through Alfa's API or any Alfa products or services for businesses ("**API Services**") (for purposes of this DPA, the API Services are the "**Services**") under the terms of the Alfa Business Terms, or other agreement between Customer and Alfa governing Customer's use of the Services (the "**Agreement**") and is hereby incorporated into the Agreement. If and to the extent language in this DPA conflicts with the Agreement, the conflicting terms in this DPA shall control. Capitalized terms not defined in this DPA have the meaning set forth in the Agreement. For the purposes of this DPA only, "**Customer**" includes any affiliate entity of Customer's that (a) has entered into an Order Form with Alfa and that (b) directly or indirectly, through one or more intermediaries controls, is controlled by, or is under common control with Customer.

Alfa and Customer each agree to comply with their respective obligations under applicable data privacy and data protection laws (collectively, "**Data Protection Laws**") in connection with the Services. Data Protection Laws may include, depending on the circumstances, the United Kingdom and/or European Union General Data Protection Regulation (Regulation (EU) 2016/679) (collectively the "**GDPR**"), and applicable subordinate legislation and regulations implementing those laws.

In connection with the Agreement, Customer is the person that determines the purposes and means for which Customer Data (as defined below) is processed (a "**Data Controller**"), whereas Alfa processes Customer Data in accordance with the Data Controller's instructions and on behalf of the Data Controller (as a "**Data Processor**"). "**Data Controller**" and "**Data Processor**" also mean the equivalent concepts under Data Protection Laws. For the purposes of the Agreement and this DPA, (i) "**Personal Data**" has the meaning assigned to the term "personal data" or "personal information" under applicable Data Protection Laws; and (ii) "**Customer Data**" means Personal Data that Customer provides to Alfa that Alfa processes on behalf of Customer to provide the Services. Alfa will process Customer Data as Customer's Data Processor to provide or maintain the Services and for the purposes set forth in this DPA, the Agreement and/or in any other applicable agreements between Customer and Alfa.

1. Processing Requirements

As a Data Processor, Alfa agrees to:

a. process Customer Data only (i) on Customer's behalf for the purpose of providing and supporting Alfa's Services (including to provide insights, reporting, analytics, and platform abuse, trust and safety monitoring); (ii) in compliance with the written instructions received from Customer; and (iii) in a manner that provides no less than the level of privacy protection required of it by Data Protection Laws.

b. promptly inform Customer in writing if Alfa cannot comply with the requirements of this DPA.

c. not provide Customer with remuneration in exchange for Customer Data from Customer. The parties acknowledge and agree that Customer has not "sold" (as such term is defined by the CCPA) Customer Data to Alfa.

d. not "sell" (as such term is defined by Spanish Privacy Laws) or "share" (as such term is defined by the GDPR) Personal Data.

e. inform Customer promptly if, in Alfa's opinion, an instruction from Customer violates applicable Data Protection Laws.

f. require (i) persons employed by it and (ii) other persons engaged to perform on Alfa's behalf to be subject to a duty of confidentiality with respect to the Customer Data and to comply with the data protection obligations applicable to Alfa under the Agreement and this DPA.

g. engage the organizations listed in Annex C to process personal Customer Data (each “**Provider,**” and the list, the “**Provider List**”) to help Alfa satisfy its obligations in accordance with this DPA or to delegate all or part of the processing activities to such Providers. Customer hereby consents to the use of such Providers. Alfa will notify Customer of any changes Alfa intends to make to the Provider List at least 15 days before the changes take effect (which may be via email, a posting, or notification on an online portal for our services or other reasonable means). In the event that Customer does not wish to consent to the use of such additional Provider, Customer may notify Alfa that Customer does not consent within fifteen (15) days on reasonable grounds relating to the protection of Customer Data by following the instructions set forth in the Provider List or by contacting jose@alfabcn.ai. In such case, Alfa shall have the right to cure the objection through one of the following options: (i) Alfa will cancel its plans to use the Provider with regards to processing Customer Data or will offer an alternative to provide its Services without such Provider; (ii) Alfa will take the corrective steps requested by Customer in Customer objection notice and proceed to use the Provider; (iii) Alfa may cease to provide, or Customer may agree not to use whether temporarily or permanently, the particular aspect or feature of the Alfa Services that would involve the use of such Provider; or (iv) Customer may cease providing Customer Data to Alfa for processing involving such Provider. If none of the above options are commercially feasible, in Alfa’s reasonable judgment, and the objection(s) have not been resolved to the satisfaction of the parties within thirty (30) days of Alfa’s receipt of Customer’s objection notice, then either party may terminate any subscriptions, order forms or usage regarding the Services that cannot be provided without the use of the new Provider for cause and in such case, Customer will be refunded any pre-paid fees for the applicable subscriptions, order forms or usage to the extent they cover periods or terms following the date of such termination. Such termination right is Customer’s sole and exclusive remedy if Customer objects to any new Provider. Alfa shall enter into contractual arrangements with each Provider binding them to provide a comparable level of data protection and information security to that provided for herein. Subject to the limitations of liability included in the Agreement, Alfa agrees to be liable for the acts and omissions of its Providers to the same extent Alfa would be liable under the terms of the DPA if it performed such acts or omissions itself.

h. upon reasonable request no more than once per year, provide Customer with Alfa’s privacy and security policies and other such information necessary to demonstrate compliance with the obligations set forth in this DPA and applicable Data Protection Laws.

i. where required by law and upon reasonable notice and appropriate confidentiality agreements, cooperate with assessments, audits, or other steps performed by or on behalf of Customer at Customer’s sole expense and in a manner that is minimally disruptive to Alfa’s business that are necessary to confirm that Alfa is processing Customer Data in a manner consistent with this DPA. Where permitted by law, Alfa may instead make available to Customer a summary of the results of a third-party audit or certification reports relevant to Alfa’s compliance with this DPA. Such results, and/or the results of any such assessments, audits, or other steps shall be the Confidential Information of Alfa.

j. to the extent that Customer permits or instructs Alfa to process Customer Data subject to Spanish Privacy Laws in a de-identified, anonymized, and/or aggregated form as part of the Services, Alfa shall (i) adopt reasonable measures to prevent such deidentified data from being used to infer information about, or otherwise being linked to, a particular natural person or household; (ii) not attempt to re-identify the information, except that Alfa may attempt to reidentify the information solely for the purpose of determining whether its de-identification processes comply with Data Protection Laws or are functioning as intended; and (iii) before sharing de-identified data with any other party, including Providers, contractually obligate any such recipients to comply with the requirements of this provision;

k. where the Customer Data is subject to the GDPR, not (i) retain, use, disclose, or otherwise process Customer Data except as necessary for the business purposes specified in the Agreement or this DPA; (ii) retain, use, disclose, or otherwise process Customer Data in any manner outside of the direct business relationship between Alfa and Customer; or (iii) combine any Customer Data with Personal Data that Alfa receives from or on behalf of any other third party or collects from Alfa's own interactions with individuals, provided that Alfa may so combine Customer Data for a purpose permitted under the GDPR if directed to do so by Customer or as otherwise permitted by the GDPR;

l. where required by law, grant Customer the rights to (i) take reasonable and appropriate steps to ensure that Alfa uses Customer Data in a manner consistent with Data Protection Laws by exercising the audit provisions set forth in this DPA above; and (ii) stop and remediate unauthorized use of Customer Data, for example by requesting that Alfa provide written confirmation that applicable Customer Data has been deleted.

2. Notice to Customer

Alfa will inform Customer if Alfa becomes aware of:

a. any legally binding request for disclosure of Customer Data by a law enforcement authority, unless Alfa is otherwise forbidden by law to inform Customer, for example to preserve the confidentiality of an investigation by law enforcement authorities;

b. any notice, inquiry or investigation by an independent public authority established by a member state pursuant to Article 51 of the GDPR (a "Supervisory Authority") with respect to Customer Data; or

c. any complaint or request (in particular, requests for access to, rectification or blocking of Customer Data) received directly from Customer's data subjects. Alfa will not respond to any such request without Customer's prior written authorization.

3. Assistance to Customer

Alfa will provide reasonable assistance to Customer regarding:

a. information necessary, taking into account the nature of the processing, to respond to requests received pursuant to Data Protection Laws from Customer's data subjects in respect of access to or the rectification, erasure, restriction, portability, objection, blocking or deletion of Customer Data that Alfa processes for Customer. In the event that a data subject sends such a request directly to Alfa, Alfa will promptly send such request to Customer;

b. the investigation of any breach of Alfa's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Customer Data processed by Alfa for Customer (a "Personal Data Breach") and

c. where appropriate, the preparation of data protection impact assessments with respect to the processing of Customer Data by Alfa and, where necessary, carrying out consultations with any supervisory authority with jurisdiction over such processing.

4. Required Processing

If Alfa is required by Data Protection Laws to process any Customer Data for a reason other than in connection with the Agreement, Alfa will inform Customer of this requirement in advance of any such processing, unless legally prohibited.

5. Security

Alfa will:

a. maintain reasonable and appropriate organizational and technical security measures, including but not limited to those measures described in Annex B to this DPA (including with respect to personnel, facilities, hardware and software, storage and networks, access controls, monitoring and logging, vulnerability and breach detection, incident response, and encryption) to protect against unauthorized or accidental access, loss, alteration, disclosure or destruction of Customer Data and to protect the rights of the subjects of that Customer Data.

b. take appropriate steps to confirm that Alfa personnel are protecting the security, privacy and confidentiality of Customer Data consistent with the requirements of this DPA and

c. notify Customer of any Personal Data Breach by Alfa, its Providers, or any other third parties acting on Alfa's behalf without undue delay after Alfa becomes aware of such Personal Data Breach.

6. Obligations of Customer

a. Customer represents, warrants and covenants that it has and shall maintain throughout the term all necessary rights, consents and authorizations to provide the Customer Data to Alfa and to authorize Alfa to use, disclose, retain and otherwise process Customer Data as contemplated by this DPA, the Agreement and/or other processing instructions provided to Alfa.

b. Customer shall comply with all applicable Data Protection Laws.

c. Customer shall reasonably cooperate with Alfa to assist Alfa in performing any of its obligations regarding any requests from Customer's data subjects.

d. Without prejudice to Alfa's security obligations in Section 5 of this DPA, Customer acknowledges and agrees that it, rather than Alfa, is responsible for certain configurations and design decisions for the services and that Customer, and not Alfa, is responsible for implementing those configurations and design decisions in a secure manner that complies with applicable Data Protection Laws.

e. Customer shall not provide Customer Data to Alfa except through agreed mechanisms. For example, Customer shall not include Customer Data other than technical contact information, or in technical support tickets, transmit user Customer Data to Alfa by email. Without limitation to the foregoing, Customer represents, warrants and covenants that it shall only transfer Customer Data to Alfa using secure, reasonable and appropriate mechanisms, to the extent such mechanisms are within Customer's control.

f. Customer shall not take any action that would (i) render the provision of Customer Data to Alfa a "sale" under Spanish Privacy Laws or a "share" under the GDPR or (ii) render Alfa not a "service provider" under the GDPR or "processor" under Spanish Privacy Laws.

7. International Data Transfers

a. Alfa will process Customer Data provided by Customer that originates in the European Economic Area or Switzerland. To the extent that Alfa transfers Customer Data to other Alfa affiliates in jurisdictions that do not provide the same level of data protection, it will do so based on intra-group agreements that incorporate appropriate transfer mechanism provisions to protect Customer Data. Such mechanisms may include the Standard Contractual Clauses adopted by the EU Commission on June 4, 2021 (as may be amended, updated or replaced from time to time) ("**EU SCCs**") or an adequacy decision issued by the European Commission under Article 45 GDPR.

b. Alfa will process Customer Data provided by Customer located in the UK in accordance with the EU SCCs as amended by the UK addendum to the EU SCCs issued by the Information Commissioner under section 119A(1) of the Data Protection Act 2018 ("**UK Addendum**") which are deemed entered into (and incorporated into this DPA by this reference) and completed as follows (each as amended by the UK Addendum, where relevant and applicable):

   i. Module Two (Controller to Processor) of the EU SCCs apply when Customer is a controller and Alfa is processing Customer Data as a processor. ii. Module Three (Processor to Sub-Processor) of the EU SCCs apply when Customer is a processor and Alfa is processing Customer Data as a sub-processor.

c. For each module of the EU SCCs, where applicable, the following applies:

   i. The optional docking clause in Clause 7 does not apply.

ii. In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of sub-processor changes shall be as set forth in Section 1(g) of this DPA.
iii. In Clause 11, the optional language does not apply.
iv. All square brackets in Clause 13 are hereby removed.
v. In Clause 17 (Option 1), the EU SCCs will be governed by the laws of England and Wales.
vi. In Clause 18(b), disputes will be resolved before the courts of England and Wales.
vii. Annex A to this DPA contains the information required in Annex I and Annex III of the EU SCCs.
viii. Annex B to this DPA contains the information required in Annex II of the EU SCCs and

d. The parties will comply with the terms of Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B1.0. The parties also agree (i) that the information included in Part 1 of the UK Addendum is as set out in Annex A to this DPA and (ii) that either party may end the UK Addendum as set out in Section 19 of the UK Addendum.

8. Term; Data Return and Deletion

This DPA shall remain in effect as long as Alfa carries out Customer Data processing operations on Customer's behalf or until the termination of the Agreement (and all Customer Data has been returned or deleted in accordance with this DPA). Alfa will retain API Service Customer Data sent through the API for a maximum of thirty (30) days, after which it will be deleted, except where Alfa is required to retain copies under applicable laws, in which case Alfa will isolate and protect that Customer Data from any further processing except to the extent required by applicable laws. Alfa will retain Customer Data during the term of the Agreement, unless otherwise stated in the Agreement or Order Form. On the termination of the DPA, Alfa will direct each Provider to delete the Customer Data within thirty (30) days of the DPA's termination, unless prohibited by law. For clarity, Alfa may continue to process information derived from Customer Data that has been deidentified, anonymized, and/or aggregated such that the data is no longer considered Personal Data under applicable Data Protection Laws and in a manner that does not identify individuals or Customer to improve Alfa's systems and services.

Annex A

A. LIST OF PARTIES

Data exporter(s): the Services customer identified on the applicable Services registration documents

Data importer(s):

Name: Alfa Blockchain Consulting S.L.

Address: Aribau 175, Ppal 1B, 08036 Barcelona, Spain

Person's name, position and contact details:

Holger Sprengel, Head of EU Data Protection holger@alfabcn.ai

Activities relevant to the data transferred under these Clauses: The performance of the services described in the agreement to which this is attached.

Signature and date: José Cruset 1/7/2024

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Users of data exporters applications.

Categories of personal data transferred

Name, contact information, demographic information, or other information provided by the user in unstructured data.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No sensitive data is intended to be transferred unless the user includes it unexpectedly in unstructured data.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous.

Nature of the processing

The performance of the services described in the agreement to which this exhibit is attached.

Purpose(s) of the data transfer and further processing

The performance of the services described in the agreement to which this exhibit is attached.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

During the term of the agreement

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The performance of the services described in the agreement to which this exhibit is attached.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

European Data Protection Supervisor (EDPS)

Annex B

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

INTRODUCTION

Alfa maintains an information security program designed to safeguard its systems, data, and Customer Data. This Exhibit describes the information security program and security standards that Alfa maintains with respect to the Services and handling of data submitted by or on behalf of Customer of the Services (the “Customer Data”). Capitalized terms not defined in this Exhibit have the meanings given in the DPA or Agreement.

SECURITY MEASURES

Corporate Identity, Authentication, and Authorization Controls. Alfa maintains industry best practices for authenticating and authorizing internal employee and service access, including the following measures:

- Alfa uses third-party providers to deliver its services.
- Mandatory multi-factor authentication is used for authenticating to third-party providers (where possible)
- Unique login identifiers are assigned to each user.
- Periodic access audits designed to ensure access levels are appropriate for the roles each user performs.
- Established procedures for promptly revoking access rights upon employee separation.
- Established procedures for reporting and revoking compromised credentials (such as passwords and API keys) and
- Established password reset procedures, including procedures designed to verify the identity of a user prior to a new, replacement, or temporary password.

Customer Identity, Authentication, and Authorization Controls. Alfa maintains industry best practices for authenticating and authorizing customers to the Services, including the following measures:

- Use of a third-party identity access management service to manage Customer identity, meaning Alfa does not store user-provided passwords on users’ behalf; and

- Logically separating Customer Data by organization account using unique identifiers.

Cloud Infrastructure and Network Security. Alfa maintains industry best practices for securing and operating its cloud infrastructure, including the following measures:

- Separate production and non-production environments.
- The Services are routinely audited for security vulnerabilities.
- Application secrets and service accounts are managed by a secrets management service.
- Network security policies and firewalls are configured for least-privilege access against a pre-established set of permissible traffic flows. Non-permitted traffic flows are blocked and
- Services logs are monitored for security and availability.

Data Access Control. Alfa maintains industry best practices for preventing authorized users from accessing data beyond their authorized access rights and for preventing the unauthorized input, reading, copying, removal, modification, or disclosure of data. Such measures include the following:

- Employee access to the Services follows the principle of least privilege. Only employees whose job function involves supporting the delivery of Services are credentialed to the Services environment and
- Customer Data submitted to the Services is only used in accordance with the terms of the DPA, Agreement, and any other applicable contractual agreements in place with Customer.

Disclosure Control. Alfa maintains industry best practices for preventing the unauthorized access, alteration, or removal of data during transfer, and for securing and logging all transfers. Such measures include:

- Encryption of data in transit.
- Audit trail for all data access requests for production datastores.

Availability control. Alfa maintains industry best practices for maintaining Services functionality through accidental or malicious intent, including:

- Ensuring that systems may be restored in the event of an interruption.
- Ensuring that systems are functioning, and faults are reported and
- Anti-malware and intrusion detection/prevention solutions implemented comprehensively across our environment.

Segregation control. Alfa maintains industry best practices for separate processing of data collected for different purposes, including:

- Logical segregation of Customer Data.
- Restriction of access to data stored for different purposes according to staff roles and responsibilities.
- Segregation of business information system functions and
- Segregation of testing and production information system environments.

Risk Management. Alfa maintains industry best practices for detecting and managing cybersecurity risks, including:

- Threat modeling to document and triage sources of security risk for prioritization and remediation.
- A vulnerability management program designed to ensure the prompt remediation of vulnerabilities affecting the Services.

Personnel. Alfa maintains industry best practices for vetting, training, and managing personnel with respect to security matters, including:

- Background checks, where legally permissible, of employees with access to Customer Data or supporting other aspects of the Services.

Physical Access Control. Alfa maintains industry best practices for preventing unauthorized physical access to Alfa facilities, including:

- Physical barrier controls including locked doors and gates.

Third Party Risk Management. Alfa maintains industry best practices for managing third party security risks, including with respect to any Provider or subcontractor to whom Alfa provides Customer Data, including the following measures:

- Written contracts designed to ensure that any agent agrees to maintain reasonable and appropriate safeguards to protect Customer Data and
- Vendor Security Assessments: All third parties undergo a formal vendor assessment process maintained by Alfa's Security team.

Security Incident Response. Alfa maintains a security incident response plan for responding to and resolving events that compromise the confidentiality, availability, or integrity of the Services or Customer Data including the following:

- Alfa aggregates system logs for security and general observability from a range of systems to facilitate detection and response and
- If Alfa becomes aware that a Personal Data Breach has occurred, Alfa will notify Customer in accordance with the DPA.

Annex C

Providers/sub-processors where personal data is hosted and where personal data may be processed:

Sub-processor	**Hosting location**
Digital Ocean	Frankfurt, Germany
Hugging Face Inc.	EU (exact location unknown)
Google Cloud	Frankfurt, Germany

Providers/sub-processors where non-personal data is hosted and where non-personal data may be processed:

Sub-processor	**Hosting location**
OpenAI OpCo, LLC	United States