Note to copy:

This Clearbit Data Processing Addendum ("DPA") is incorporated into the Clearbit Terms of Service available at https://clearbit.com/legal.

For Customers that would like to receive a signed copy of the Clearbit DPA, we have made this copy available to you. This copy includes signatures on the Data Processing Addendum version last modified March 1, 2024, followed by our Technical and Organizational Security Measures and a complete copy of the Standard Contractual Clauses and UK Addendum, which are incorporated by reference within the DPA. No changes made to this copy are agreed to by APIHub, Inc. dba Clearbit or its affiliates.

Please note that we update the DPA as described in the "General Provisions" section below.

If you have any questions, please contact your Clearbit representative.

CLEARBIT DATA PROCESSING ADDENDUM

1. Introduction

This Clearbit Data Processing Addendum ("DPA") amends and is incorporated into the agreement between Clearbit and Customer, and will be applicable to each party's Processing of Personal Data, where such Processing is regulated by Data Protection Laws. Except for the changes made by this DPA, the agreement remains unchanged and in full force and effect. In the event of a conflict between this DPA and any other portion of the agreement, the provision of this DPA shall control. The parties agree that this DPA shall replace any existing data processing terms the parties may have previously entered into in connection with the Clearbit Services and will be applicable when either party Processes Personal Data where such Processing is regulated by Data Protection Laws.

Capitalized terms have the meaning given to them in the agreement, unless otherwise defined below.

2. Definitions

For the purpose of this DPA:

"Business Contact Data" means all Personal Data or other materials provided or collected by you in connection with the Clearbit Services.

"Business Contact Data Business Purposes" means the improvement, development, provision and enhancement of the Clearbit Services.

"California Personal Information" means Processor Data that is subject to the protection of the CCPA.

"CCPA" means California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020).

“Consumer,” “Business,” “Sell,” “Service Provider,” and “Share” will have the meanings given to them in the CCPA.

“Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

“Controller Data” means any Personal Data that either party provides to the other party as separate, independent Controllers in the course of Clearbit providing the Services to Customer, including Product Data and Business Contact Data.

“Data Privacy Framework” means the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework and the UK Extension to the EU-U.S. Data Privacy Framework self-certification programs (as applicable) operated by the U.S. Department of Commerce; as may be amended, superseded or replaced.

“Data Privacy Framework Principles” means the Principles and Supplemental Principles contained in the relevant Data Privacy Framework; as may be amended, superseded or replaced.

“Data Protection Laws” means all applicable worldwide legislation relating to data protection and privacy which applies to the respective party in the role of Processing Personal Data in question under the agreement, including without limitation European Data Protection Laws, the CCPA, the Telephone Consumer Protection Act, the CAN-SPAM Act of 2003 and other applicable U.S. federal and state privacy laws, in each case as amended, repealed, consolidated or replaced from time to time.

“Data Subject” means the individual to whom Personal Data relates.

“Europe” means the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom.

“European Data” means Personal Data that is subject to the protection of European Data Protection Laws.

“European Data Protection Laws” means data protection laws applicable in Europe, including: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (“GDPR”); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (“ePrivacy Directive”); and (iii) applicable national implementations of (i) and (ii); (iii) GDPR as it forms parts of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 (“UK GDPR”); and (iv) Swiss Federal Data Protection Act and its Ordinance (“Swiss DPA”); in each case, as may be amended, superseded or replaced.

“Instructions” means the written, documented instructions issued by a Controller to a Processor, and directing the same to perform a specific or general action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion and making available).

“Permitted Affiliates” means any of your Affiliates that (i) are permitted to use the Clearbit Services pursuant to the agreement but have not entered their own separate agreement with us,

(ii) qualify as a Controller of Personal Data Processed by us, and (iii) are subject to European Data Protection Laws.

“Personal Data” means any information relating to an identified or identifiable individual where such information is protected as personal data, personal information, or personally identifiable information under applicable Data Protection Laws.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Processor Data transmitted, stored or otherwise Processed by us and/or our Sub-Processors in connection with the provision of the Clearbit Services. “Personal Data Breach” will not include unsuccessful attempts or activities that do not compromise the security of Processor Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

“Processing” means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data. The terms “Process”, “Processes” and “Processed” will be construed accordingly.

“Processor” means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

“Processor Data” means any Personal Data provided or otherwise made available by Customer or on Customer's behalf to Clearbit in its capacity as a Processor in connection providing the Services to Customer.

“Standard Contractual Clauses” means the standard contractual clauses annexed to the European Commission’s Decision (EU) 2021/914 of 4 June 2021 currently found at https://eur-lex.europa.eu/eli/dec_impl/2021/914, as may be amended, superseded or replaced.

“Sub-Processor” means any Processor engaged by us or our Affiliates to assist in fulfilling our obligations with respect to the Processing of Processor Data under the agreement. Sub-Processors may include third parties or our Affiliates but will exclude any Clearbit employee or consultant.

“UK Addendum” means the International Data Transfer Addendum issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018 currently found at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf, as may be amended, superseded or replaced.

3. Roles of the parties

3.1. The parties acknowledge and agree that:

a. with respect to the Processing of Controller Data, each of the parties are separate, independent Controllers and will comply with their respective obligations under Data Protection Laws when Processing Controller Data; and

b. with respect to the Processing of Processor Data, Customer is the Controller and Clearbit is a Processor acting on behalf of Customer.

3.2. For clarity, nothing in the agreement or this DPA shall restrict Clearbit in any way from its ability to access, use, share, or store Personal Data that Clearbit would otherwise Process independently of Customer's use of the Clearbit Services.

4. Data Processing

4.1. The categories of Data Subjects affected by the Processing of Personal Data within scope of this DPA will be business contacts or prospects of Customer and visitors to Customer's websites or digital properties. The types of Personal Data affected by the Processing within the scope of this DPA will include business contact information (which may include name, work email address, title and work phone number) and electronic activity data (which may include IP address, cookie identifiers, other online identifiers and website activity data) of Data Subjects. The Personal Data transferred will be subject to the following basic processing activities: to provide the Clearbit Services and to facilitate the Customer's Permitted Uses of the Clearbit Services and Clearbit's Business Contact Data Business Purposes.

5. Customer Responsibilities

5.1. You will be responsible for complying with all requirements that apply to you under applicable Data Protection Laws with respect to your Processing of Personal Data and the Instructions you issue to us. In particular but without prejudice to the generality of the foregoing, you acknowledge and agree that you will be solely responsible for: (i) the accuracy, quality, and legality of Personal Data that you provide to us and the means by which you acquired such Personal Data; (ii) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of such Personal Data, including obtaining any necessary consents and authorizations; (iii) ensuring you have the right to transfer, or provide access to, such Personal Data to us for Processing in accordance with the agreement (including this DPA); and (iv) ensuring that your Instructions to us regarding the Processing of Processor Data comply with applicable laws, including Data Protection Laws. You will inform us without undue delay if you are not able to comply with your responsibilities under this Section or Data Protection Laws.

6. Product Data

6.1. Each party acknowledges and agrees that: (a) Product Data is made available to Customer solely for the limited and specified purpose(s) of enhancing business contact data for Customer's sales and marketing purposes; (b) with regards to its Processing of Product Data, Customer shall comply with and provide the same level of privacy protection as is required by the CCPA; (c) Clearbit shall have the right, upon reasonable notice, to take reasonable and appropriate steps to (1) ensure that Customer uses Product Data in a manner consistent with Clearbit's obligations under Data Protection Laws and (2) stop and remediate unauthorized uses of Product Data; (d) if requested by Clearbit, Customer shall attest that it Processes Product Data in compliance with Data Protection Laws; and (e) Customer shall notify Clearbit promptly if Customer determines it can no longer meet its obligations under Data Protection Laws.

7. Business Contact Data

7.1. Each party further acknowledges and agrees that Business Contact Data may be made available by Customer to Clearbit for the Business Contact Data Business Purposes. Customer

makes Business Contact Data available for Clearbit's Business Contact Data Business Purposes, and Clearbit shall Process Business Contact Data for the Business Contact Data Business Purposes. For clarity, Clearbit may receive the same Business Contact Data from multiple customers or through Clearbit's own data collection methods ("Duplicate Business Contact Data"), and Clearbit is not restricted in any way under the agreement from its access, use, sharing or storage of such Duplicate Business Contact Data.

8. Cooperation

8.1. If either party receives any complaint, notice or communication from a supervisory authority or other governmental authority which relates to the other party's: (a) Processing of the Personal Data; or (b) potential failure to comply with Data Protection Laws with respect to the Processing ofPersonal Data, that party shall direct the supervisory authority or governmental authority to the other party and, in the case of intertwined obligations, claims, or Personal Data at issue, shall provide reasonable assistance to the other party in responding to the supervisory authority or governmental authority.

9. International Transfers

9.1. Data Transfers: You acknowledge and agree that we may access and Process Personal Data on a global basis as necessary to provide the Clearbit Services in accordance with the agreement, and in particular that Personal Data may be transferred to and Processed by Clearbit in the United States and to other jurisdictions where Clearbit Affiliates and Sub-Processors have operations. Wherever Personal Data is transferred outside its country of origin, each party will ensure such transfers are made in compliance with the requirements of Data Protection Laws.

9.2. Cross-Border Data Transfers: With respect to transfers of European Data from one party to the other party in any country not recognized as providing an adequate level of protection for Personal Data (within the meaning of applicable European Data Protection Laws), the Standard Contractual Clauses will be incorporated by reference and form part of the agreement as follows:

9.2.1. (i) Module 1 applies to the transfer of Controller Data between the parties as Controllers, Module 2 applies to the transfer of Processor Data from Customer to Clearbit and Module 3 applies to the transfer of Processor Data to the extent the Customer is a Processor of European Data; (ii) in Clause 7, the optional docking clause applies; (iii) in Clause 9, Option 2 applies and changes to Sub-Processors will be notified in accordance with the 'Sub-Processors' section of this DPA; (iv) in Clause 11, the optional language is deleted; (v) in Clauses 17 and 18, the parties agree that the governing law and forum for disputes for the Standard Contractual Clauses will be the Republic of Ireland; (vi) the Annexes of the Standard Contractual Clauses will be deemed completed with the information set out in the Schedules of this DPA; (vii) the supervisory authority that will act as competent supervisory authority will be determined in accordance with GDPR; and (viii) if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA, the Standard Contractual Clauses will prevail to the extent of such conflict.

9.2.2. In relation to European Data that is subject to the UK GDPR, the Standard Contractual Clauses will apply in accordance with sub-section (a) and the following modifications: (i) the Standard Contractual Clauses will be modified and interpreted in accordance with the UK Addendum, which will be incorporated by reference and form an

integral part of the agreement; (ii) Tables 1, 2 and 3 of the UK Addendum will be deemed completed with the information set out in the Schedules of this DPA and Table 4 will be deemed completed by selecting “neither party;” and (iii) any conflict between the terms of the Standard Contractual Clauses and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

9.2.3. In relation to European Data that is subject to the Swiss DPA, the Standard Contractual Clauses will apply in accordance with sub-section (a) and the following modifications: (i) references to “Regulation (EU) 2016/679” will be interpreted as references to the Swiss DPA; (ii) references to “EU,” “Union” and “Member State law” will be interpreted as references to Swiss law; and (iii) references to the “competent supervisory authority” and “competent courts” will be replaced with the “the Swiss Federal Data Protection and Information Commissioner” and the “relevant courts in Switzerland.”

9.2.4. In the event that Clearbit certifies to the Data Privacy Framework for European Data, Clearbit will rely on the Data Privacy Framework (instead of the Standard Contractual Clauses) to lawfully receive European Data in the United States, and Clearbit will ensure that it provides at least the same level of protection to such European Data as is required by the Data Privacy Framework Principles and notify Customer know if it is unable to comply with this requirement.

10. Processor Data

10.1. Compliance with Instructions: We will only Process Processor Data for the purposes described in this DPA or as otherwise agreed within the scope of your lawful Instructions, except where and to the extent otherwise required by applicable law. We are not responsible for compliance with any Data Protection Laws applicable to you or your industry that are not generally applicable to us. If we believe that your Instruction infringes Data Protection Laws (where applicable), we will inform you without delay. Customer shall have the right, upon notice, to take reasonable and appropriate steps to (i) ensure that Clearbit uses Processor Data in a manner consistent with Customer's obligations under Data Protection Laws, or (ii) stop and remediate unauthorized Processing of Processor Data.

10.2. Conflict of Laws: If we become aware that we cannot Process Processor Data in accordance with your Instructions due to a legal requirement under any applicable law, we will (i) promptly notify you of that legal requirement to the extent permitted by the applicable law; and (ii) where necessary, cease all Processing (other than merely storing and maintaining the security of the affected Processor Data) until such time as you issue new Instructions with which we are able to comply. If this provision is invoked, we will not be liable to you under the agreement for any failure to perform the applicable Clearbit Services until such time as you issue new lawful Instructions with regard to the Processing.

10.3. Controller Instructions: The parties agree that the agreement (including this DPA), together with your use of the Clearbit Services in accordance with the agreement, constitute your complete Instructions to us in relation to the Processing of Processor Data, so long as you may provide additional instructions during the term of the Subscription that are consistent with the agreement and the nature and lawful use of the Clearbit Services.

10.4. Confidentiality: We will ensure that any personnel whom we authorize to Process Processor Data on our behalf is subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to that Processor Data.

10.5. Technical and Organizational Measures: Clearbit shall implement and maintain appropriate technical and organizational measures to provide a level of security appropriate to the risk for the Processing of Processor Data, as described in Schedule 1 to Addendum A of this

DPA. Clearbit shall regularly test, assess, and evaluate the effectiveness of such technical and organizational measures for ensuring the security of the Processing.

10.6. Personal Data Breach: We will notify you without undue delay after we become aware of any Personal Data Breach and will provide timely information relating to the Personal Data Breach as it becomes known or reasonably requested by you. At your request, we will promptly provide you with such reasonable assistance as necessary to enable you to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if you are required to do so under Data Protection Laws.

10.7. Sub-Processors: Where Clearbit engages Sub-Processors, Clearbit agrees to (i) enter into a written agreement with Sub-Processors that imposes on Sub-Processors data protection and security requirements for Processor Data that comply with Data Protection Laws and provide at least the same level of protection for Processor Data as those in this DPA; and (ii) remain responsible to Customer for Sub-Processors' compliance with the obligations of this DPA and for any acts or omissions of Sub-Processors that cause Clearbit to breach any of its obligations under this DPA.

10.8. Sub-Processors List: Customer authorizes Clearbit to engage Sub-Processors to Process Processor Data on behalf of Customer, as listed at https://clearbit.com/subprocessors. If Clearbit engages any additional or replacement Sub-Processors, Clearbit will give Customer notice at least 30 calendar days in advance of providing that Sub-Processor with access to Processor Data. If Customer does not provide timely objection to a new Sub-Processor, Customer will be deemed to have authorized Clearbit's use of the new Sub-Processor and waived its right to object. If Customer provides timely objection to a new Sub-processor, the parties will discuss Customer's concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, Clearbit will, at its sole discretion, either not appoint the new Sub-Processor, or permit Customer to suspend or terminate the affected Service in accordance with the termination provisions of the Agreement without liability to either party (but without prejudice to any fees incurred by Customer prior to suspension or termination).

10.9. Audits: Upon request, Clearbit will make available to Customer all reasonable information necessary, and allow for and contribute to audits, including inspections, conducted by Customer, or another auditor who is not a competitor and agreed to in advance by Clearbit, to demonstrate compliance with this DPA. Such audits or inspections shall be limited to Clearbit's Processing of Processor Data in its capacity as a Processor only, not any other aspect of Clearbit's business or information systems. If Customer requires Clearbit to submit to audits or inspections that are necessary to demonstrate compliance with this DPA, Customer will provide Clearbit with written notice at least sixty (60) days in advance of such audit or inspection. Such written notice will specify the people, places, or documents to be made available. Any information produced by Clearbit in response to an audit request will be considered Clearbit's Confidential Information and, notwithstanding anything to the contrary in the Agreement, will remain Confidential Information. Customer will make every effort to cooperate with Clearbit to schedule audits or inspections at times that are convenient to Clearbit during usual business hours and without disturbance to Clearbit's operations and personnel. Customer shall be solely responsible for all costs incurred in relation to audits or inspections.

10.10. Data Subject Requests: Clearbit agrees to comply with all reasonable instructions from Customer related to any requests from individuals exercising their rights in Personal Data granted to them under Data Protection Laws ("Privacy Request"). At Customer's request and without undue delay, Clearbit agrees to reasonably assist Customer in answering or complying

with any Privacy Request.
10.11. Cooperation: Clearbit will cooperate to the extent legally required in connection with Customer's obligation to conduct data protection impact assessments and engage in consultations with supervisory authorities regarding its Processing of Processor Data. If a supervisory authority corresponds with Clearbit regarding its Processing of Processor Data under the agreement, Clearbit will promptly notify Customer and cooperate to the extent reasonably necessary for Customer to respond to the supervisory authority's request. Customer will bear the costs that Clearbit incurs when fulfilling such obligations.
10.12. Return and Deletion of Processor Data: Processor Data (including any copies) shall not be kept longer than is required to provide the Clearbit Services under the agreement, unless (i) a longer retention period is required to comply with applicable laws, including for audit, legal, financial, or regulatory purposes; or (ii) Customer instructs Clearbit in writing to (a) keep certain Processor Data longer, or (b) return certain Processor Data earlier.
10.13. Additional Provisions for California Personal Information: This Section of the DPA will apply only with respect to California Personal Information.

10.13.1. Roles of the Parties: When processing California Personal Information in accordance with your Instructions, the parties acknowledge and agree that you are a Business and we are a Service Provider for the purposes of the CCPA.

10.13.2. Responsibilities: We certify that we will Process California Personal Information as a Service Provider strictly for the purpose of performing the Clearbit Services under the agreement (the "Business Purpose") or as otherwise permitted by the CCPA. Further, we certify we (i) will not Sell or Share California Personal Information; (ii) will not Process California Personal Information outside the direct business relationship between the parties, unless required by applicable law; and (iii) will not combine the California Personal Information included in Customer Data with personal information that we collect or receive from another source (other than information we receive from another source in connection with our obligations as a Service Provider under the agreement). 10.13.3. CCPA Compliance: We will (i) comply with obligations applicable to us as a Service Provider under the CCPA and (ii) provide California Personal Information with the same level of privacy protection as is required by the CCPA. Customer shall have the right, upon notice, to take reasonable and appropriate steps to (i) ensure that Clearbit uses California Personal Information in a manner consistent with Customer's obligations under the CCPA, or (ii) stop and remediate unauthorized Processing of California Personal Information. We will notify you if we make a determination that we can no longer meet our obligations as a Service Provider under the CCPA.

10.13.4. CCPA Audits: You will have the right to take reasonable and appropriate steps to help ensure that we use California Personal Information in a manner consistent with Customer's obligations under the CCPA. Upon notice, you will have the right to take reasonable and appropriate steps in accordance with the agreement to stop and remediate unauthorized use of California Personal Information.

10.13.5. Not a Sale: The parties acknowledge and agree that the disclosure of California Personal Information by the Customer to Clearbit does not form part of any monetary or other valuable consideration exchanged between the parties.

11. General Provisions
11.1. Amendments: Notwithstanding anything else to the contrary in the Agreement, we reserve the right to make any updates and changes to this DPA.
11.2. Severability: If any individual provisions of this DPA are determined to be invalid or

unenforceable, the validity and enforceability of the other provisions of this DPA will not be affected.

11.3. Limitation of Liability: Each party and each of their Affiliates' liability, taken in aggregate, arising out of or related to this DPA (including any other DPAs between the parties) and the Standard Contractual Clauses, where applicable, whether in contract, tort or under any other theory of liability, will be subject to the limitations and exclusions of liability set out in the 'Limitations of Liability' section of the agreement and any reference in such section to the liability of a party means aggregate liability of that party and all of its Affiliates under the agreement (including this DPA).

11.4. Permitted Affiliates: By entering the agreement, you agree to this DPA (including, where applicable, the Standard Contractual Clauses) on behalf of yourself and in the name and on behalf of your Permitted Affiliates. For the purposes of this DPA only, and except where indicated otherwise, the terms “Customer,” “you” and “your” will include you and such Permitted Affiliates.

11.5. Authorization: The legal entity agreeing to this DPA as Customer represents that it is authorized to agree to and enter into this DPA for and on behalf of itself and, as applicable, each of its Permitted Affiliates.

11.6. Remedies: The parties agree that (i) solely the Customer entity that has entered the agreement will exercise any right or seek any remedy any Permitted Affiliate may have under this DPA on behalf of its Affiliates, and (ii) the Customer entity that has entered the agreement will exercise any such rights under this DPA not separately for each Permitted Affiliate individually but in a combined manner for itself and all of its Permitted Affiliates together. The Customer entity that has entered the agreement is responsible for coordinating all Instructions, authorizations and communications with us under the DPA and will be entitled to make and receive any communications related to this DPA on behalf of its Permitted Affiliates.

EXECUTED BY THE PARTIES’ AUTHORIZED REPRESENTATIVES:

APIHub, Inc. dba Clearbit, by and on behalf of its affiliates, as applicable.

Signature: Scott Mendelson
9BA90D4B2134495...

Name: Scott Mendelson

Title: Senior Director, Sales

Controller: _____

Signature: _____

Name: _____

Title: _____

Date: _____

Schedule 1 to Addendum A

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Clearbit reserves the right to update its security program from time to time; provided, however, any update will not materially reduce the overall protections set forth in this Schedule.

1. Compliance

Clearbit will comply with all applicable state and federal data security regulations and shall abide by all required security controls as stated herein, based upon the nature of the Services provided, the data involved and/or the location where such Services are rendered.

2. Security Certification

Clearbit holds the following security-related certifications from independent third-party auditors: SOC 2 Type II.

3. Information Security Program

Clearbit maintains a formal information security program that is supported by written information security policies, approved by management, published, and communicated to staff. The information security program is based on a recognized security framework designed to protect the confidentiality and integrity of data, and appropriate to the nature, scope, context and purposes of processing and the risks involved in the processing for the data subjects.

4. Organization of Information Security

Clearbit will delegate an accountable party for information security intended to provide oversight and approval for security and compliance initiatives and planning through various actions. The delegate(s) will be required to review, recommend edits or changes, and accept internal information security policy and processes.

5. Access Control

Clearbit shall have in place formal processes and procedures to support the secure creation, amendment, and deletion of user accounts of personnel, consultants, and subcontractors, as well as systems and software, which contain, or otherwise have access to European Data. Furthermore, Clearbit takes it upon itself to carry out the following measures:

- Monitor redundant and inactive accounts
- Ensure that all user accounts privileges are allocated on “a-need-to-use-basis”
- Ensure that access control mechanisms based on reasonably secure passwords are enforced
- Ensure, where possible, Clearbit’s internal system access authentication is using two-factor authentication

6. Data Center Architecture and Security

Data centers must be designed and managed in compliance with regulations, standards, and best practices, such as SOC 2, PCI DSS Level 1, ISO 27001, CSA and FIPS 140-2. The data center must implement physical and environmental controls designed to secure the facility and

protect equipment from damage. Clearbit must exercise regular oversight of the data center supplier's ability to meet these controls by reviewing current independent third-party reports of compliance and/or industry standard certifications.

7. Network Architecture and Security

Clearbit networks must span multiple availability zones that are physically separated and isolated, connected through low-latency, high-throughput, and highly redundant networking. Networks or applications that contain Customer data must be separated from public networks by a firewall to prevent unauthorized access from the public network.

8. Availability and Continuity

a. Service Availability. Clearbit employs service clustering and network redundancies to eliminate single points of failure. Clearbit maintains a publicly available system-status webpage, which includes system availability details, scheduled maintenance, and service incident history, found at: https://clearbit.statuspage.io/.

b. Backups. European Data is backed up daily using policy-based scheduling.

c. Disaster Recovery and Business Continuity. Clearbit has a disaster recovery plan that outlines roles and responsibilities for key personnel involved in business continuity, our plan to activate and respond to a disaster, target timelines and testing requirements.

9. Information Security Incident Management

Clearbit will have a documented incident response plan that is approved by management. The key components must include:

- Classify the severity of the incident using an initial analysis
- Limit the immediate impact of the incident
- Take corrective action to contain the impact
- Investigate and collect evidence
- Inform the relevant authorities (where applicable)
- Inform impacted customers

10. Software Development

Clearbit shall have appropriate governance processes in place to supervise and monitor software development (e.g., implement an SDLC) and ensure information security requirements are included in the requirements for new information systems or enhancements to existing information systems.

11. Security Testing

At least quarterly vulnerability scanning will be performed against all public-facing applications. At least annually, Clearbit will engage a third-party security expert to perform a penetration test. Critical and high-risk vulnerabilities identified during the scanning will be promptly remediated.

12. Personnel Security

Clearbit performs pre-employment background checks of all personnel with exposure to Customer data, in accordance with applicable local laws. These personnel must receive security

training upon hire and at least annually thereafter. Personnel must be bound by written confidentiality agreements.

13. Encryption Controls
Clearbit implements reasonable measures to ensure data cannot be read, copied, modified, or removed without authorization during electronic transmission or transport. Data is encrypted in transit over public networks via industry standard HTTPS/TLS (TLS 1.2 or higher).

Data at rest is encrypted in storage in databases, storage buckets and backup files using AES-256-bit encryption.

14. Additional Technical and Organizational Security Measures
a. Measures of encryption of personal data. Clearbit has taken the following measures in the Clearbit Services designed to convert clearly legible European Data into ciphertext by means of a cryptographic process:

1. European Data transmitted via TLS can be encrypted with TLS 1.2 or stronger protocol.
2. European Data at rest is encrypted by default using AES256 or a stronger alternative.

b. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services.

1. Clearbit has taken the following measures designed to ensure that European Data is accessed only by authorized personnel and prevents the intrusion by unauthorized persons into Clearbit's systems and applications used for the processing of European Data:

• Two factor or two-step authentication is required.
• All European Data is subject to the encryption measures identified above.
• Development and test environments are logically separated from production environments by design.
• Clearbit maintains administrative controls which govern access under the principle of least privilege.
• Privileged access is not granted by default.

2. Clearbit has taken the following measures designed to ensure that European Data cannot be read, copied, modified, or removed without authorization during electronic transmission or transport, and that it is possible to check and establish whether and by whom European Data has been input into data processing systems, modified, or removed:

• All European Data is subject to the encryption measures identified above.
• Clearbit must maintain tools in place for audit trails, event notifications, and logs for application and cloud systems.

3. Clearbit has taken the following measures designed to ensure that European Data is protected from accidental destruction or loss due to internal or external influences, and ensure the ability to withstand attacks or to quickly restore systems to working order after an attack):

• Alerting is set up for specified thresholds and a team with experienced personnel monitors system availability and overall health.
• High availability infrastructure is used as appropriate to increase availability.
• Clearbit ensures routine backups are taken of European Data.

c. Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident. Clearbit has taken the following measures designed to ensure the possibility to quickly restore the Clearbit system or European Data in the event of a physical or technical incident:

• Clearbit maintains an incident response plan that it updates from time to time as needed. The incident response plan includes procedures for handling and reporting incidents including detection and reaction to possible Security Incidents.
• Capacity management measures are taken to monitor resource consumption of systems as well as plan future resource requirements.

d. Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing. Clearbit has taken the following measures designed to ensure the regular review and assessment of security measures:

• Clearbit conducts regular penetration testing and vulnerability scanning of the Services.
• Clearbit must maintain a channel to allow security researchers to report identified security vulnerabilities in the Services.

e. Measures for user identification and authorization. Clearbit has taken the following measures designed to validate and authenticate users:

• Clearbit maintains administrative controls which govern access under the principle of least privilege.
• Access to non-public data or functionality requires authentication prior to access.
• Two factor or two-step authentication is required.

f. Measures for the protection of data during transmission. Clearbit has taken the following measures designed to ensure transmission control to ensure that European Data cannot be read, copied, changed, or deleted without authorization during its transfer and that European Data can be monitored and determined to which recipients a transfer of European Data is intended:

• European Data is encrypted in transit as described above.

g. Measures for the protection of data during storage. Clearbit has taken the following control measures designed to ensure that European Data cannot be read, copied, changed, or deleted without authorization while stored on data media:

• European Data is encrypted at rest as described above.
• Two factor or two-step authentication is required.

h. Measures for ensuring physical security of locations at which personal data are processed. Clearbit has taken the following measures regarding the physical security of European Data:

• Physical access within data processing facilities is controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means.

i. Measures for ensuring events logging. Clearbit has taken the following measures designed to ensure the verifiability of event log files:

• Clearbit records application and system logs to collect information, exception errors, information security events and privileged access events.
• Clearbit maintains administrative controls which govern access under the principle of least privilege.

j. Measures for ensuring system configuration, including default configuration. Clearbit has taken the following measures designed to ensure that all in-scope systems and devices are compliant with baseline configuration settings:

• Clearbit ensures that access to information and application system functions is restricted to authorized personnel only.

k. Measures for internal IT and IT security governance and management. Clearbit has a dedicated and identified person to oversee its information security and compliance program. Clearbit is annually audited by an independent third-party against an industry standard (e.g. SOC 2 Type II, ISO 27001, etc.).

l. Measures for certification/assurance of processes and products. Clearbit is annually audited by an independent third-party against an industry standard (e.g. SOC 2 Type II, ISO 27001, etc.).

m. Measures for ensuring data minimization. Clearbit has taken the following measures designed to reduce the amount of data collected by the Service:

• Clearbit will implement capabilities for the Customer to customize which data is collected by the Service, where practical.

n. Measures for ensuring data quality. Clearbit has taken the following measures designed to ensure that the data flow creates and sustains good data quality:

• Clearbit has established processes for data subjects to exercise their data protection rights (right to amend and update information).
• Clearbit's documentation clearly states the types of data Customer is prohibited from transferring to Clearbit.

o. Measures for ensuring limited data retention. Clearbit has established processes designed to ensure that European Data is deleted in accordance with the terms of the agreement following the termination of the agreement.

p. Measures for ensuring accountability. Clearbit has an appointed Data Protection Officer or another similar role who is responsible for overseeing Clearbit's compliance with its legal and contractual privacy-related obligations throughout the data lifecycle.

q. Measures for allowing data portability and ensuring erasure. Clearbit has established processes in relation to the exercise by users of their privacy rights (including without limitation, rights of data portability and erasure).

[END OF PAGE]

Schedule 2 to Addendum A

STANDARD CONTRACTUAL CLAUSES - INTRODUCTION & SUPPLEMENTAL TERMS

ANNEX I

DETAILS OF PROCESSING

Exhibit 1A (Processor Modules)

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

- Data exporter: Customer
    - Name: As set forth in the Customer's Clearbit Account (on behalf of itself and Permitted Affiliates)
    - Address: As set forth in the Customer's Clearbit Account
    - Contact person’s name, position and contact details, including email: As set forth in the Customer's Clearbit Account
    - Activities relevant to the data transferred under these Clauses: Processing of Processor Data in connection with Customer's use of the Clearbit Services under the agreement.
    - Signature and date: Customer is deemed to have signed this Annex I by accepting the agreement.
    - Role (controller/processor): Controller (either as the Controller; or acting in the capacity of a Controller, as a Processor, on behalf of another Controller)
- Data importer: Clearbit
    - Name: APIHub, Inc. dba Clearbit
    - Address: 548 Market St #95879 San Francisco, CA 94104-5401
    - Contact details: privacy@clearbit.com
    - Activities relevant to the data transferred under these Clauses: Processing of Processor Data in connection with Customer's use of the Clearbit Services under the agreement.
    - Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

- Categories of data subjects whose personal data is transferred: Individuals located in Europe and associated or potentially associated with business organizations.

- Categories of personal data transferred: Business contact information including, but not limited to, first and/or last name, business address, business email address, business phone number, employer, business role, professional title, and other similar information.
- 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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: No sensitive data transferred.
- 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 nature of the processing includes but is not limited to collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data, whether or not by automated means.
- Purpose(s) of the data transfer and further processing: To provide Clearbit Services pursuant to the agreement, as further specified in the Order and as further instructed by Customer.
- The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: For the duration of the Subscription Term of the agreement, unless (i) a longer retention period is required for audit, legal or regulatory purposes.
- For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: For the duration of the agreement or as otherwise agreed upon in writing or required by applicable law.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

For purposes of Clause 13, Customer agrees the competent supervisory authority will be the Data Protection Commission (DPC) of Ireland.

Exhibit 1B (Controller Module)

A. LIST OF PARTIES
MODULE ONE: Transfer controller to controller

- Data importer/exporter: Customer
    - Name: As set forth in the Customer's Clearbit Account (on behalf of itself and Permitted Affiliates)
    - Address: As set forth in the Customer's Clearbit Account

- Contact person's name, position and contact details, including email: As set forth in the Customer's Clearbit Account
- Activities relevant to the data transferred under these Clauses: Processing in connection with the receipt of the Clearbit Services provided by the data importer.
- Signature and date: Customer is deemed to have signed this Annex I by accepting the agreement.
- Role (controller/processor): controller

- Data importer/exporter: Clearbit
  - Name: APIHub, Inc. dba Clearbit
  - Address: 548 Market St #95879 San Francisco, CA 94104-5401
  - Contact details: privacy@clearbit.com
  - Activities relevant to the data transferred under these Clauses: Processing in connection with the receipt of the Clearbit Services provided by the data importer.
  - Role (controller/processor): controller

B. DESCRIPTION OF TRANSFER

MODULE ONE: Transfer controller to controller

- Categories of data subjects whose personal data is transferred: Individuals located in Europe and associated or potentially associated with business organizations.
- Categories of personal data transferred: Business contact information including, but not limited to, first and/or last name, business address, business email address, business phone number, employer, business role, professional title, and other similar information.
- 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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: No sensitive data transferred.
- 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 nature of the processing includes, but is not limited to, collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data, whether or not by automated means.
- Purpose(s) of the data transfer and further processing: The provision of the Clearbit Services contemplated in the agreement, including the Customer's Permitted Uses of the Clearbit Services, and for Clearbit's Business Contact Data Business Purposes.

- The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: For the duration of the Subscription Term of the agreement, unless a longer retention period is required for audit, legal or regulatory purposes.
- For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: For the duration of the agreement or as otherwise agreed upon in writing or required by applicable law.

C. COMPETENT SUPERVISORY AUTHORITY
MODULE ONE: Controller to Controller

For purposes of Clause 13, Customer agrees the competent supervisory authority will be the Data Protection Commission (DPC) of Ireland.

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

MODULE ONE: Transfer controller to controller
MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons. The description of technical and organizational measures designed to ensure the security of Processor Data is set out in Schedule 1 to Addendum A.

For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter. The description of technical and organizational measures designed to ensure the security of Processor Data is set out in Schedule 1 to Addendum A.