Idera Affiliates Data Processing Terms

(for the Customer-Facing DPA)

Details of Processing of Apilayer Data Products GmbH

a. **Address:**

13-15 / 6. Floor.
Untere Donaustraße
1020 Vienna, Austria

b. **Type of Services provided by Apilayer involving the Processing of Customer Personal Data:**

Apilayer is the leading provider of off-the-shelf, cloud-based API products built to help developers and businesses around the world operate quickly and effectively. Apilayer addresses this demand with highly reliable and scalable APIs that can be configured fast and require minimal maintenance.

c. **Data Protection Officer (DPO) Details:**

VeraSafe, LLC, a Delaware limited liability company.
experts@verasafe.com

d. **EU Data Protection Representative:**

n/a

e. **UK Data Protection Representative:**

VeraSafe United Kingdom Ltd.
37 Albert Embankment London SE1 7TL United Kingdom
Contact form: https://verasafe.com/public-resources/contact-data-protection-representative

f. **Subject matter and duration:**

The subject matter and duration of the Processing of Customer Personal Data are set forth in the Main Agreement and all amendments, exhibits, schedules, task orders, addenda, SOWs, purchase orders and other documents associated therewith and incorporated therein.

g. **Nature and Purpose of Processing:**

The nature and purpose of the Processing of Customer Personal Data are set forth in the Main Agreement and all amendments, exhibits, schedules, task orders, addenda, SOWs, purchase orders and other documents associated therewith and incorporated therein.

h. **Further Processing:**

No further Processing of Customer Personal Data beyond the Processing necessary for the provision of the Services is allowed.

i. **Categories of Data Subjects:**

Data subjects may include Customer's representatives, such as employees, contractors, collaborators, partners. Data subject may also include individuals attempting to communicate or transfer Customer Personal Data to users of the Services.

j. **Categories of Customer Personal Data:**

The Categories of Customer Personal Data that Customer authorizes and requests that Apilayer's Processes include but are not limited to: Personal contact information such as full name, address, mobile number, email address; details including employer name, job title and function, identification numbers and business contact details; goods or services provided; IP addresses and interest data.

k. **Special Categories of Customer Personal Data to be Processed (if applicable) and the applied restrictions to the Processing of these Special Categories of Customer Personal Data:** n/a

l. **Categories of third-party recipients to whom the Customer Personal Data may be disclosed or shared by Idera:**

Subprocessors; and

Other Idera Affiliates, if applicable.

m. **Frequency of the Transfer of Customer Personal Data:**

The frequency of the transfer of Customer Personal Data is determined by the Customer. Customer Personal Data is transferred each time that the Customer instructs Apilayer to Process Customer Personal Data.

n. **Maximum data retention periods, if applicable:**

The retention period of the Customer Personal Data is generally determined by the Customer, and is subject to the term of the DPA and the Main Agreement, respectively, in the context of the contractual relationship between Apilayer and the Customer.

o. **The basic Processing activities to which Customer Personal Data will be subject include, without limitation:**

Collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction for the purpose of providing the Services to Customer in accordance with the terms of the Main Agreement.

p. **The following is deemed an instruction by the Customer to Apilayer to Process Customer Personal Data:**

(a) Processing in accordance with the Main Agreement.

(b) Processing initiated by Data Subjects in their use of the Services.

(c) Processing to comply with other reasonable documented instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Main Agreement.

q. **List of Apilayer's Subprocessors: https://www.ideracorp.com/Legal/APILayer/Subprocessors**

r. **Description of technical and organizational security measures implemented by the Apilayer:**

i. Measures of pseudonymization and encryption of Customer Personal Data:

(a) Encryption of the transferred Customer Personal Data in transit using the Transport Layer Security (TLS) protocol version 1.2 or higher with a minimum of 128-bit encryption; and

(b) Encryption at rest within Apilayer’s software applications using a minimum of AES-256.

ii. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of Processing systems and services:

(a) Restriction of logical access to IT systems that Process transferred Customer Personal Data to those officially authorized persons with an identified need for such access;
(b) Active monitoring and logging of network and database activity for potential security events, including intrusion;
(c) Regular scanning and monitoring of any unauthorized software applications and IT systems for vulnerabilities of Apilayer;
(d) Firewall protection of external points of connectivity in Data Importer’s network architecture; and
(e) Expedited patching of known exploitable vulnerabilities in the software applications and IT systems used by Apilayer.

iii. Measures for ensuring the ability to restore the availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident:

The AWS RDS instance is governed by robust replication policies that ensure data snapshots are available for restoration or in the case of performance scaling purposes.

iv. Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the Processing:

All deployments made across any accounts or environments includes a double secret decryption step, ensuring both the DevOps user performing the action and all systems in use are authenticated during any CI/CD process or any request made by customer api service or internal service to system call.

Regular expiry of any IT and DevOps MFA tokens enforces regular re-authentication or session refresh by all users.

v. Measures for user identification and authorization:

Customer access to API services via HTTP request is governed by request authorization headers that include a provisioned token and data defining the accounts access to features. This request data is never passed to any actual service but is instead consumed by APILayer’s API Gateway. The token governs the expiry, access, etc.

Customer Account access granted through product portals is governed by username and password per portal, per account.

All AWS hosted system credentials are doubly encrypted at the account level and the username level. Root AWS access is not granted to individuals, and all root keys + secrets are doubly encrypted at the account and username levels.

vi. Measures for the protection of data during transmission:

Transport from request origin, through API Gateway, and underlying services is locked down entirely through AWS access policies and doubly encrypted secrets for all database / account access across the systems.

vii. Measures for the protection of data during storage:

APILayer AWS RDS instances utilize the AWS RDS at-rest policy of AES-256 bit encryption.

viii. Measures for ensuring physical security of locations at which Customer Personal Data are processed:

Restriction of physical to IT systems that Process transferred Customer Personal Data to those officially authorized persons with an identified need for such access.

ix. Measures for ensuring events logging:

Active monitoring and logging of network and database activity for potential security events, including intrusion.

Active monitoring and logging of internal network and database activity for potential security events, including intrusion.

Active monitoring of api service health, request activity, threat identification, errors, performance by Sentry IO SDK.

x. Measures for ensuring system configuration, including default configuration:

All systems configurations are governed by secret/key associations, preventing invalid or unauthorized configurations from integration. Regular monitoring and logging of system connections E2E.

xi. Measures for internal IT and IT security governance and management:

Root accounts are double encrypted at account and username levels. Secret decryption requires user accounts to have a valid MFA session and appropriate AWS access policy to assume the role for the account to which access is requested.

xii. Measures for certification/assurance of processes and products:

SSL certification managed by IDERA IT policy.

Aforementioned account access by process, systems, and product services is controlled by secret / key encryption and decryption for assurance of identity validation.

Users are required to adhere to MFA token recycling on local machines and any AWS console login via CLI or web interface.

xiii. Measures for ensuring data minimization:

Data minimization is guaranteed during the design and implementation processes.

xiv. Measures for ensuring data quality:

Customer is responsible for data quality and accuracy since the data is provided by the Customer.

Form validations are made to validate some fields.

xv. Measures for ensuring limited data retention:

Different policies can apply depending on the type of data. Where applicable, temporary data storage is facilitated by AWS S3 services.

xvi. Measures for ensuring accountability:

Account access through processes, across systems, and E2E product services is controlled by secret / key encryption and decryption for assurance of identity validation.

Users are required to adhere to MFA token recycling on local machines and any AWS console login via CLI or web interface.

xvii. Measures for allowing data portability and ensuring erasure:

AWS RDS policy ensures migrations, backups, and instance erasure operations are available at authorized user (IT/DevOps) behest.

xviii. Other:

(a) Internal policies establishing that

i. Where Apilayer is prohibited by law from notifying Data Exporter of an order from a public authority for transferred Customer Personal Data, Apilayer shall take into account the laws of other jurisdictions and use best efforts to request that any confidentiality requirements be waived to enable it to notify the competent Supervisory Authorities;

ii. Apilayer must require an official, signed document issued pursuant to the applicable laws of the requesting third party before it will consider a request for access to transferred Customer Personal Data;

iii. Apilayer shall scrutinize every request for legal validity and, as part of that procedure, will reject any request Data Importer considers to be invalid; and

iv. If Apilayer is legally required to comply with an order, it will respond as narrowly as possible to the specific request.