Idera Affiliates Data Processing Terms

(for the Customer-Facing DPA)

Details of Processing of Filestack, Inc.

a. Address:

4001 W. Parmer Lane, Suite 125, Austin, TX 78727

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

Filestack powerful APIs enable developers to process content at scale and provide an off-the-shelf tech stack from uploading, transforming, understanding, and delivering content within applications and interfaces. Filestack's low-code platform enables developers to build automated content processing and analysis that dramatically accelerates the development lifecycle. The company's infrastructure powers billions of file uploads, transformations, and downloads every month for customers in a wide variety of industries, including ed-tech, e-commerce, crowdsourcing, and printing.

c. Data Protection Officer (DPO) Details:

VeraSafe, LLC

experts@verasafe.com

100 M Street S.E., Suite 600, Washington, D.C . 20003 USA

d. EU Data Protection Representative:

VeraSafe Ireland Ltd.
Unit 3D North Point House North Point Business Park New Mallow Road, Cork T23AT2P Ireland
Contact form: https://verasafe.com/public-resources/contact-data-protection-representative

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 Filestack 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 Filestack 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 Filestack 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 Filestack 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 Filestack's Subcontractors** is available at **https://www.ideracorp.com/legal/filestack/subprocessors.**

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

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

a. Customer creates and manages encryption keys. The AWS platform enforces the customer to maintain an encrypted password.
b. Customer encrypts data before transmission.
c. Data transmissions to Filestack hosts are through secure HTTP with TLS 1.2 (only strong cipher suites accepted).
d. Data transmissions within Filestack infrastructure are through secure protocols.
e. Customer Scoped Data stays encrypted throughout Filestack infrastructure.
f. Customer Scoped Data stays encrypted at rest.
g. No Filestack employee has customer's encryption keys.

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 Filestack;

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 Filestack.

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:

a. RTO: 24 hours

b. RPO: 12 hours

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

a. Software development security test performed daily

b. Software build vulnerability scans are performed regularly.

c. SOC 2 audit performed yearly (independent party)

d. Application Penetration Tests are performed yearly (independent party)

e. Internal security audit is performed yearly

v. Measures for user identification and authorization:

a. User Access Policy established

b. User Access are reviewed when one of the following events occurs:

1. Major change in organization structure
2. Major change in security architecture
3. Major attrition
4. Security incident
5. Twice a year

vi. Measures for the protection of data during transmission:

a. Customer creates and manages encryption keys

b. Customer encrypts data before transmission

c. Data transmissions to Filestack hosts are through secure HTTP with TLS 1.2 (only strong cipher suites accepted)

d. Data transmissions within Filestack infrastructure are through secure protocols.

e. Customer Scoped Data stays encrypted throughout Filestack infrastructure.

vii. Measures for the protection of data during storage:

a. Customer Scoped Data stays encrypted at rest.

b. No Filestack employee has customer's encryption keys.

c. Access to network assets is restricted to a small Operations Team's members.

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

a. Filestack does not have data centers; all servers are hosted via AWS.

ix. Measures for ensuring events logging:

a. All systems and network assets are monitored 24/7. Alert rules are configured to create alert events for any anomaly or unauthorized activities. IDS/IPS service is setup for all critical network assets.

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

a. All systems and network assets are built by codes. Baseline default configurations are embedded in deployment codes.

b. Code modifications must go through Filestack standard Change Management Process.

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

a. IT/IS Security Policy and Procedure established.

b. All IT personnel are required to complete yearly security and compliance training.

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

a. Software build vulnerability scans are performed regularly.

b. Application Penetration Tests are performed yearly.

c. SOC 2 Type 2 audit performed yearly.

d. Internal security audits are performed yearly.

xiii. Measures for ensuring data minimization:

a. N/A. Filestack does not collect, retain, or use any of Customer Scoped Data.

xiv. Measures for ensuring data quality:

a. N/A. Filestack does not collect, retain, or use any of Customer Scoped Data.

xv. Measures for ensuring limited data retention:

a. N/A. Filestack does not collect, retain, or use any of Customer Scoped Data .

xvi. Measures for ensuring accountability:

a. Each authorized access is unique and traceable.

b. Authorized access is reviewed quarterly.

c. System audit logs are retained for 180 days.

xvii. Measures for allowing data portability and ensuring erasure:

a. Customer data is stored on AWS.

b. Customers have the option of storing their data (documents, images, etc.) on the Filestack AWS servers. The contents of the data are determined by the customer (Filestack has no control over the contents of the files). The customer controls when data is deleted).

i. Other:

(a) Internal policies establishing that

i. Where Filestack is prohibited by law from notifying Data Exporter of an order from a public authority for transferred Customer Personal Data, Filestack 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. Filestack 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. Filestack 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 Filestack is legally required to comply with an order, it will respond as narrowly as possible to the specific request.