Data Processing Addendum

This Data Processing Addendum (this "**Addendum**") is an addendum to the Terms of Service at https://www.filestack.com/terms, as it may be updated from time to time, or other agreement between Filestack, Inc. ("**Filestack**") and the Filestack customer (the "**Customer**") for Filestack's services (the "**Services Agreement**").

This Addendum includes the following parts: **(i)** the main body of the Addendum; **(ii)** Schedule 1 –Europe Specific Terms, including Appendix 1 to Schedule 1 – Processing Details, and **(iii)** Schedule 2 – Description of Filestack's Technical and Organizational Security Measures.

1. **Definitions**. The following words have the meaning stated when used in this Addendum. Capitalized terms not otherwise defined in this Addendum have the meanings stated in the Services Agreement.

   applicable law means: **(i)** laws generally applicable to personal data and the provision of the Services in the jurisdiction where the personal data is processed; and **(ii)** if applicable, the Directive or GDPR (as of the date the GDPR becomes applicable), and the Swiss Federal Act on Data Protection.

   data subject means an individual natural person that is identified or identifiable by means of the personal data;

   disclose means to disclose or give access to;

   GDPR means the European Union General Data Protection Regulation (EU) 2016/679;

   law means statutes, regulations, executive orders, and other rules issued by a government office or agency that have binding legal force;

   personal data means any information about a natural person that is identified or identifiable to the natural person, either alone or in combination with other information, that Filestack will process or have access to as part of providing the Services, including any such information that is created by means of the Services. Personal data includes "personal data" at that term is defined in the Directive and GDPR;

   personnel means the employees and individual contractors under the direct supervision of the person referred to;

   process when used with respect to data means: (i) to record, store, organize, structure, analyze, query, modify, combine, encrypt, display, disclose, transmit, receive, render unusable, or destroy, by automated means or otherwise, and (ii) to provide cloud or other remote technology hosting services for applications or services that do any of the foregoing, and (iii) any other use or activity that is defined or understood to be processing under applicable law. The terms process, processing and their variants should be construed broadly in light of the parties' goal to protect personal data;

   security event means any of the following: (i) unauthorized processing or other use or disclosure of personal data, (ii) unauthorized access to or acquisition of personal data or the systems on which personal data is processed; (ii) any significant corruption or loss of personal data that Filestack is unable to repair within a minimal period of time, (iii) any event that has or is reasonably likely to

significantly disrupt the processing of the personal data as contemplated by the Services Agreement, and (iv) any material unsuccessful attempt to gain unauthorized access to, or to destroy or corrupt, the personal data, but not including any routine, unsuccessful events such as pings, port scans, blocked malware, failed login attempts, or denial of service attacks;

sensitive personal data means (a) information regarding an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, sex life, or sexual orientation; (b) all or part of a social security number, passport number, driver's license number, or similar identifier; (c) genetic data, biometric data, and health information; (d) account passwords or other credentials other than as needed to use the Filestack Services; (e) date of birth; (g) criminal history; (h) mother's maiden name; and (i) any other information that is a special category of data under applicable law;

sub-processor and sub-processor agreement have the meaning given in Section 4 (*Disclosure to Third Parties*) below;

third party means any natural person or legal person other than Filestack, Customer, or either of their personnel.

2. General. Filestack shall comply with the requirements stated in this Addendum, and any additional or more stringent requirements or restrictions under applicable law. On Customer's request Filestack shall execute one or more additional data transfer and processing agreements in a form required or recognized under applicable law for international transfers of personal data, to include any standard clauses published pursuant to applicable law, such as the Standard Contractual Clauses published by the European Commission. Customer acknowledges that the Filestack service does not include a notice or consent process for Customer's compliance with its obligations as a data controller under applicable law. For example, the Filestack service authenticates Customer's users via a stored token. Customer is responsible for any notice and consent requirements in connection with this authentication process and any other process that enables its users' personal data to be processed by Filestack.

3. Permitted Use and Disclosure. Filestack shall not process personal data except as follows:

(i) as necessary to provide the Services in accordance with the Services Agreement, subject to Section 4 (*Disclosure to Third Parties*);

(ii) as required by applicable law, subject to Subsection 4.2 (*Legally Required Disclosure*); and

(iii) as necessary to comply with legal requirements for records retention or for internal administrative purposes related to the provision of the Services, except to the extent such processing would violate restrictions under applicable law.

For clarity, Filestack may not aggregate the personal data with other data, or process, access, or use the personal data for any purpose not expressly authorized above.

4. Disclosure to Third Parties.

4.1 Disclosure to Sub-processors. Filestack may disclose Customer's personal data to a permitted subcontractor (a "sub-processor") as necessary for the sub-processor to provide the subcontracted part of the Services, provided that: (i) Filestack has conducted appropriate due diligence to confirm that the sub-processor is capable of providing the level of protection for personal data that is required by the Services Agreement and this Addendum; (ii) the sub-processor is subject to written obligations to protect the personal data at least as stringent as those stated in this Addendum, including all notice and audit terms (each a "sub-processor agreement"). Filestack shall be responsible for the acts and omissions of each sub-processor in violation of this Addendum to the same extent as for Filestack's own acts and omissions.

4.2 Legally Required Disclosures. Filestack may disclose personal data as required by a subpoena or other compulsory legal process provided that: (i) it gives Customer as much advance notice of the disclosure as is reasonably practical under the circumstances (unless notice is prohibited by law), (ii) it discloses only the personal data that it is legally compelled to disclose, in the reasoned, written opinion of Filestack's counsel, and (iii) it cooperates, at Customer's expense, with Customer's reasonable requests to avoid or limit disclosure, or if Filestack is not permitted to give notice of the disclosure, it uses reasonable efforts to challenge or narrow the requirement in accordance with applicable law.

4.3 Requests from Data Subjects. Filestack shall promptly notify Customer if Filestack receives a request from a data subject to disclose, provide a copy, modify, block, or take any other action with respect to the personal data, unless notice is prohibited by applicable law. Filestack shall not independently take any action in response to a request from a data subject without Customer's prior written instruction. Filestack shall cooperate with Customer's reasonable requests for access to personal data and other information and assistance as necessary to respond to a request or complaint by a data subject.

5. Protection of Personal Data. Filestack shall protect the personal data from unauthorized acquisition, use, disclosure, loss, corruption, and unavailability using those physical, technical, organizational, and administrative safeguards described on Schedule 2. Filestack will require its sub-processors to use safeguards at least as protective of the personal data as the safeguards applicable to Filestack.

6. Notice of Security Event. Filestack shall provide prompt notice to Customer's technical and account contacts using those means established for routine account-related communications if Filestack opens an "incident" or otherwise begins a formal process to investigate a suspected security event. Filestack shall provide notice as provided in Section 13.2 (*Notices*) without undue delay and all events within forty-eight (48) hours of discovering that a security event has occurred. A security event is "discovered" under this Section at the time it is actually discovered, or at any earlier time that the Filestack should have discovered the security event given the safeguards required by Section 5 (*Protection of Personal Data*). Filestack's notice shall include the following information to the extent it is reasonably available to Filestack at the time of the notice, and Filestack shall update its notice as additional information becomes reasonably available: (i) the dates and times of the security event; (ii) the facts that underlie the discovery of the security event, or the decision to begin an investigation into a suspected security event, as applicable; (iii) a description of the personal data involved in the security event, either

specifically, or by reference to the data set(s), and (iv) the measures planned or underway to remedy or mitigate the vulnerability giving rise to the security event. Filestack shall promptly provide other information regarding the security event or suspected security event that Customer may reasonably request.

7. Mitigation/Investigation/Remediation. Filestack shall take those measures available, including measures reasonably requested by Customer, to address a vulnerability giving rise to a successful security event, both to mitigate the harm resulting from the security event and to prevent similar occurrences in the future. Filestack shall cooperate with Customer's reasonable requests in connection with the investigation and analysis of the security event, including a request to use a third- party investigation and forensics service. Filestack shall retain all information that could constitute evidence in a legal action arising from the security event and shall provide the information to Customer on Customer's request. Except to the extent required by law in the written and reasonable opinion of Filestack's counsel, Filestack shall not disclose to any person the existence of a security event or suspected security event or any related investigation without Customer's prior written consent.

8. Cooperation. Filestack shall cooperate with Customer's reasonable requests for information and assistance in connection with (i) Customer's internal security and privacy assessments, and (ii) any audits or verifications of Customer's privacy and security policies and practices by Customer's customers, regulators, or other stakeholders.

9. Business Continuity Plan. Filestack shall maintain a written business continuity/disaster recovery plan (a "BCP") to enable Filestack to timely recover and resume its operations in the event of a disruptive event, including an event that would constitute "*force majeure*" event as described in the Services Agreement. Filestack shall test its BCP at least annually, in accordance with the terms of the Plan. On Customer's request, Filestack will provide a summary of its BCP, or will provide Customer and its auditors with controlled access to the full BCP, provided that the auditors are subject to confidentiality terms at least as stringent as those stated in the Agreement.

10. Records and Audit. Filestack shall keep reasonable records to evidence its compliance with this Addendum, and shall preserve the records for at least two (2) years from the date of the events reflected in the records. Filestack shall provide Customer or its independent third-party auditor with access to its relevant records, systems, facilities and personnel for the purpose of auditing or verifying compliance with this Addendum, provided that any such audit or verification shall be performed on reasonable advance notice and shall not unduly disrupt Filestack's operations. If any audit or verification reveals a failure to comply with any requirement set forth in this Addendum, Filestack shall promptly provide a plan to remediate the failure and begin remediation. Filestack shall bear all reasonable costs for controlled re-verification of the remediation of any such issue

11. Return or Destruction of personal data. On expiration of the Services Agreement or any earlier termination, or on Customer's request at any time, Filestack shall return or destroy any personal data that is within its control; provided, however, that:

(i) on Customer's request, Filestack shall not destroy the personal data until it has given Customer access to the personal data for a reasonable period of time as necessary to complete an orderly migration of the personal data to Customer's or a substitute provider's systems;

(ii) if Customer requires Filestack to return or destroy personal data prior to the expiration or termination of the Services Agreement, Filestack is excused from performing those Services that it is unable to perform as a result of the return or destruction; and

(iii) Filestack is not required to return or destroy personal data to the extent it is expressly permitted to retain the personal data under Section 2 (*Permitted Use and Disclosure*) above, or if destruction or return is commercially or technically infeasible. Filestack shall provide a written description of any personal data that it proposes to retain with a statement of the reasons for retention, and shall cooperate with Customer's reasonable requests to address record keeping needs or to overcome infeasibility issues. On Customer's request, Filestack shall provide a certification (signed by its executive offer) that return or destruction has been completed in accordance with this Addendum.

12. Customer Obligations. Customer makes the following representations, warranties, and covenants: (i) the personal data has been collected in accordance with applicable law, including requirements for notices and consents legally required for Filestack to access and process the personal data in accordance with the Services Agreement; (ii) the transfer of the personal data to Filestack for the purpose of Filestack providing the Services is authorized under applicable law; (iii) Customer shall comply with applicable law as to requests from data subjects in connection with the personal data; (iv) Customer shall disclose to Filestack only that personal data that is necessary for Filestack to provide the Services in accordance with the Services Agreement; (v) Customer shall not ask Filestack to take any action with respect to the personal data the Customer is not permitted to take directly; (vi) the personal data does not include any sensitive personal data, and (vii) Customer shall indemnify and hold harmless Filestack from any and all claims, losses, or damages (including reasonable attorney fees, costs and regulatory fines) arising from Customer's breach of this Section.

13. General.

13.1 Term and Termination. This Addendum is effective as of the Effective Date and shall continue in effect for so long as Filestack continues to have access to or process personal data. This Addendum survives the expiration or termination of the Services Agreement for so long as Filestack has access to or processes personal data. If Filestack violates this Addendum, Customer may terminate this Agreement and the Services Agreement for breach. Customer may, in its sole discretion, give Filestack an opportunity to cure any violation, and may suspend Filestack's access to or processing of the personal data during the cure period.

13.2 Notices. Except as otherwise expressly stated otherwise in this Addendum, notices required under this Addendum shall be given in writing in the manner required in the Services Agreement. If Customer has provided a privacy notice contact, Filestack shall also notify Customer's privacy notice contact.

13.3 Precedence and Interpretation. This Addendum is intended to supplement the Services Agreement. If there is a conflict between this Addendum and the Services Agreement, this Addendum controls. If there is a conflict between the terms of Schedule 1 to this Addendum and the body of this Addendum, Schedule 1 controls. Any ambiguity in this Addendum as to a matter covered by applicable law should be interpreted in a way that conforms to applicable law.

13.4 Rights in Data. As between Customer and Filestack, Customer retains all right, title and interest in and to the personal data.

13.5 Assignment, Change in Control. Filestack must give Customer advance written notice of any transaction that will result in a change of control of Filestack or any sub-processor, or assignment or transfer of this Agreement or any sub-processor agreement. If Customer reasonably concludes that the following the transaction the Filestack or its successor does not have the operational or financial strength to perform the Filestack's obligations under this Agreement, Customer may terminate the Services Agreement without liability. The requirements of this Subsection are in addition to any requirements stated in the Services Agreement and apply notwithstanding anything to the contrary in the Services Agreement.

13.6 Confidential Information. Any additional or more stringent protections or remedies available with respect to information defined as "confidential information" or with like term under the Services Agreement apply to personal data.

Filestack, Inc.	ChurchSuite Ltd
Slawomir Zabkiewicz	Gavin Courtney
Name: Slawomir Zabkiewicz	Name: Gavin Courtney
Title: Chief Architect	Title: Managing Director
Date Signed: 09 / 02 / 2020	Date Signed: 07 / 26 / 2021

Attach: Schedule 1 (Europe Specific Terms)

Schedule 1 Europe Specific Terms

This Schedule 1, Europe Specific Terms states additional requirements and restrictions applicable to Filestack's processing of personal data that is covered by the Directive, or the GDPR as of the date that the GDPR becomes effective as to the personal data, and the Swiss Federal Act on Data Protection (the "**Applicable European Law**"). Terms used in this Schedule 1 that are defined in the Directive or GDPR have the meaning given in the Directive or GDPR, as applicable. The "personal data" referred to below refers only to the personal data that Filestack will have access to or will process pursuant to the Services Agreement.

1. **Legal Relationship to Personal Data**. The parties acknowledge that Customer is the "controller" and Filestack is a processor, or that Customer is a "processor" and Filestack is a "sub-processor." The processing details of the Services and the categories of personal data are described on Appendix 1 to this Schedule 1.

2. **Cross-Border Transfer of Personal Data**. The parties contemplate that Customer will transfer the personal data covered by this Schedule 1 to Filestack's services environment located in the United States. Transfer to and from the U.S. is made via global networks managed by Filestack's content management sub-processors and may entail temporary storage outside of the U.S. With respect to this transfer, Customer is the "exporter" and Filestack is the "importer" of the personal data covered by this Schedule 1. Filestack has certified its adherence to the EU-US and US-Swiss Privacy Shield Framework as administered by the U.S. Department of Commerce, and will maintain the certification for the term of the Services Agreement. Filestack will provide at least the level of privacy protection required by the Privacy Shield principles. The standard contractual clauses for the transfer of personal data to processors established in third countries under the Directive and the GDPR or its national equivalents "**Standard Contractual Clauses**") are attached to this Schedule 1 as Appendix 2 and are incorporated in this Schedule 1 by this reference. If there is a conflict between the Standard Contractual Clauses and this DPA, the Standard Contractual Clauses shall control.

3. **Further Transfer**. Filestack shall not further transfer the personal data outside of the United States, or give access to the personal data to any person (natural person or entity) outside of the United States or to any international organization except: (i) as described on Appendix 1 to this Schedule 1; (ii) as expressly authorized in writing by Customer, or (iii) as required by Applicable European Law, provided that Filestack has first given Customer reasonable advance notice of the transfer or access, unless such notice is prohibited by Applicable European Law.

4. **Addendum General Terms**. Reference is made to the restrictions and requirements stated in the Data Processing Addendum to which this Schedule 1 is attached. This Schedule 1 is not intended to be the entire statement of Filestack's obligations with respect to the processing of the personal data, but to supplement those obligations with respect to the personal data covered by this Schedule 1 such that Filestack has fully documented its obligations with respect to the implementation of appropriate technical and organizational measures to protect data subjects in compliance with Applicable European Law.

5. **Processing**. Filestack will keep personal data confidential and only process personal data to the extent necessary to perform the Services in accordance with the Services Agreement and in accordance with Customer's written instructions. Filestack will not process Customer's personal data for any other purpose unless Customer specifically authorizes such purpose in writing.

6. **Sub-processors**. Filestack shall use sub-processors only as expressly permitted by the Services Agreement. Filestack shall provide information regarding the sub-processors as the Customer may reasonably request. Before engaging a sub-processor, Filestack shall perform reasonable diligence to discover if the sub-processors have the operational and financial strength to comply with the Addendum and this Schedule 1 and shall document its findings. Filestack shall ensure that all sub-processors are subject to written, legally binding obligations that: (i) protect the confidentiality or the personal data to at least the same extent as required by the Addendum and this Schedule 1; (ii) require the implementation of those technical and organizational measures required by the Addendum and this Schedule 1 to the extent those measures are applicable or appropriate to the processing or access by the sub-processor; (iii) require sub-processor to provide assistance and information to Filestack in connection with Filestack's obligation to provide assistance and information under Section 9 (*Assisting Data Controller*) below; and (iv) require the sub-processor to comply with the same obligations of Filestack stated in the Addendum and this Schedule 1 as to any engagement with another processor. Filestack acknowledges that it remains responsible to the Customer for each sub-processor's compliance with the requirements of the Addendum and this Schedule 1.

7. **Changes to Sub-processors**. Filestack shall maintain a list of Sub-processors on a Customer-accessible Web page. If Customer subscribes to Filestack's update service for Sub-processors, Filestack will provide notice to Customer each time that it updates the list of Sub-processors. If Filestack plans to add or change any sub-processors during the term of the Services Agreement, it shall provide Customer with written notice in advance of the change such that Customer has a reasonable opportunity to review the new sub-processor. If Customer reasonably objects to a new sub-processor on the grounds that it is not able to protect the personal data to the standards required by this Addendum and Schedule 1, then Customer may terminate the Agreement without liability.

8. **Security**. Filestack will implement and maintain the technical, physical, administrative and organizational measures to protect personal data against theft, unauthorized or unlawful acquisition, access, or processing, accidental loss, destruction, alteration, or damage as described in Section 5 (*Protection of Personal Data*) of the Addendum, as well as any other minimum security requirements required by laws generally applicable to processors.

9. **Assisting Data Controller**. Filestack shall provide reasonable assistance as Customer (or the controller, if other than Customer) shall reasonably request in connection with the controller's obligation to respond to requests for exercising the data subject's rights under Applicable European Law, taking into account the nature of the processing and the information available to the processor. Customer acknowledges that Filestack does not have a means of identifying files within Customer's account to specific Customer users, and that Customer is responsible for

implementing a means of tracking files that include personal data to enable compliance with requests from data subjects for erasure, amendment, or other action.

10. **Data Return or Destruction**. Filestack shall comply with the requirements of the Services Agreement, the Addendum, and this Schedule 1 (including the requirements of Schedule 2) with regards to the return or destruction of the personal data.

11. **Records, Demonstrating Compliance**. In addition to the record keeping requirements stated in the Services Agreement and the Addendum, Filestack will keep written records of the processing activities described on Appendix 1 to this Schedule 1 as required by Applicable European Law and shall make those records available to Customer, the controller if other than Customer, and the controller's supervisory authority, on request. Filestack shall cooperate with Customer's reasonable requests to otherwise document and demonstrate compliance with Applicable European Law, and shall allow for and contribute to audits, including inspections, conducted by Customer, the controller, if other than Customer, or another auditor mandated by the controller. Customer shall comply with the requests of the controller's supervisory authority in the performance of its tasks. Customer acknowledges that Filestack's disclosure of information to the controller, an auditor, or the controller's supervisory authority pursuant to this Section does not constitute a breach of any confidentiality obligations stated in the Services Agreement, the Addendum, or this Schedule 1 so long as Filestack has used reasonable efforts to provide notice of the disclosure as far in advance as is practical, unless notice is prohibited by Applicable European Law.

12. **Notice of Data Breach**. Filestack shall notify Customer without undue delay after becoming aware of a personal data breach. The notification shall include, at a minimum, all of the following information to the extent it is known to Filestack, and Filestack shall supplement the notice to the extent the following information is learned or discovered by Customer after the initial notice: (i) a description of the nature of the personal data breach, including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (ii) the name and contact details of Customer's data protection officer or other contact point where more information can be obtained; (iii) the likely consequences of the personal data breach (iv) the measures taken or proposed to be taken by Filestack to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

13. **Customer's Obligations**. Customer makes the following representations, warranties, and covenants: (i) the personal data has been collected in accordance with Applicable European Law and Customer (or the controller, if other than Customer) has complied with applicable legal requirements necessary to authorize Filestack to perform the processing in accordance with the Services Agreement, including any cross-border transfer of the personal data; (ii) Customer shall comply with all requirements of Applicable European Law applicable to it as a processor, or controller, as applicable, such as the requirements to comply with certain requests from data subjects in connection with the personal data; (iii) Customer shall disclose to Filestack only that personal data that is necessary for Filestack to provide the Services in accordance with the

Services Agreement; (iv) Customer shall not ask Filestack to take any action with respect to the personal data the Customer is not permitted to take directly; and (v) Customer shall indemnify and hold harmless Filestack from any and all claims, losses, or damages (including reasonable attorney fees, costs and regulatory fines) arising from Customer's breach of this Section.

Data Processing Addendum, Schedule 1, Appendix 1
Processing Details

Purpose of Processing:

To provide the Services described in the Terms of Service, namely file upload and conversion services

Categories of data subjects:

Individuals whose personal data is included in files that Customer transmits to Filestack for processing.

Categories of personal data:

Any personal data included in files that Customer transmits to Filestack for processing.

Categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations:

Sub-processors described in Section 6 of the Addendum; Filestack's personnel in EU member countries may have access to personal data.

Third countries or international organizations to which the personal data will be transferred, if applicable:

Transfer to and from the U.S. via global networks managed by importer's content management sub-processors that may entail temporary storage outside of the U.S.

Technical and Organizational Security Measures

See Schedule 2 attached to the Addendum.

Data Processing Addendum, Schedule 1, Appendix 2

Standard Contractual Clauses for Processors

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organisation: ChurchSuite Ltd

Address: Floor 2, 1 Broadway, Nottingham, NG1 1PR

Tel.: +441158242300 ; fax: ; e-mail: support@churchsuite.com

Other information needed to identify the organisation:

(the data **exporter**)

And

Name of the data importing organisation: Filestack, Inc.

Address: 122 E. Houston Street, San Antonio, Texas 78205

Tel.: 1-888-415-1885 ; fax: ; e-mail: privacy@filestack.com

Other information needed to identify the organisation: n/a

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1 to Attachment 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or

accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any

of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same

conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full): Gavin Courtney

Position: Managing Director

Address: Floor 2, 1 Broadway, Nottingham, NG1 1PR

Other information necessary in order for the contract to be binding (if any):

Signature:

Gavin Courtney

On behalf of the data importer:

Name (written out in full): Slawomir Zabkiewicz

Position: Chief Architect

Address: 122 E. Houston Street, San Antonio, Texas 78205

Other information necessary in order for the contract to be binding (if any): n/a

Signature:

Slawomir Zabkiewicz

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Provider of online services used by organisations to facilitate the organisation, planning and communication with their members and supporters.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Provider of online services used by providers to upload, transform, deliver and manage files within their applications.

Data subjects

Exporter personnel whose personal data is provided to importer for the purposes of establishing and maintaining the exporter's account;

Individuals whose personal data may be part of a processed file or may be included in the metadata associated with the file.

Categories of data

Name, business contact information, business IP address, service account names and passwords, and tokenized social media platform authentication information of exporter personnel who are assigned by exporter to manage the exporter's accounts with importer;

Files; other personal data that the exporter may elect to include as part of the file metadata associated with the file.

Special categories of data (if appropriate)

The personal data transferred concern may include the following special categories of data (please specify):

Importer does not require sensitive data for purposes of providing the services, but importer does not control the content of the images or associated file data processed by means of its services, so sensitive data may appear in files or metadata associated with the files.

Processing operations

The personal data transferred will be subject to one or more the following basic processing activities (please specify):

Transfer to and from the U.S. via global networks managed by importer's content management sub-processors that may entail temporary storage outside of the U.S.

Processing as necessary to provide the importer's services in accordance with the service agreement between exporter and importer.

DATA EXPORTER

Name: Gavin Courtney

Authorised Signature:

Gavin Courtney

DATA IMPORTER

Name: Slawomir Zabkiewicz

Authorised Signature

Slawomir Zabkiewicz

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Those measures described in Schedule 2 of the Data Processing Addendum between Exporter and Importer.

Privacy Addendum, Schedule 2
Description of Filestack's Technical and Organizational Security Measures

- Authentication and authorization
    - User account assignment
    - User-level privileges
    - Multi-factor authentication
    - ID/password security procedures
- Data Protection
    - All customer data is stored in USA
    - Internal policies and procedures
    - Differentiated access rights (profiles, roles, transactions and objects)
    - Encryption at rest
- Cloud infrastructure security
    - All servers hosted in Amazon AWS
    - Physical and environment controls provided by Amazon AWS
    - Datacenter and physical security by Amazon AWS
- Network and infrastructure security
    - Fully authenticated and authorized sessions
    - End-to-end encryption using TLS 1.2
    - Cryptographically verifiable client certificates
    - Role and attribute based access controls
    - Configurable user and device access policies
    - Event-based audit trail
    - All servers in virtual private cloud with network access control lists and bastion hosts
- Encryption
    - Encrypted data transmission
    - TLS vulnerabilities monitoring
    - Data encryption at rest
    - Key management encryption
- Business continuity and operational resilience
    - Multi zone and multi region infrastructure with Amazon AWS
    - Service monitoring
    - Communication and reporting
- Security incident management
    - Incident response plan
    - Incident response team
    - Breach notification

HELLOSIGN

Audit Trail

TITLE	Filestack Data Processing Addendum
FILE NAME	FileStack DPA (sz 2020 09 02).docx
DOCUMENT ID	b1b0cc38b66bed75bfd14301bfa0897be3c3a076
AUDIT TRAIL DATE FORMAT	MM / DD / YYYY
STATUS	Completed

Document History

VIEWED	**07 / 26 / 2021** 11:10:37 UTC	Viewed by - (gavin@churchsuite.com) IP: 82.14.45.46
SIGNED	**07 / 26 / 2021** 11:15:59 UTC	Signed by - (gavin@churchsuite.com) IP: 82.14.45.46
COMPLETED	**07 / 26 / 2021** 11:15:59 UTC	The document has been completed.