FrontApp Data Processing Addendum

This Data Processing Addendum ("**DPA**") is entered into between FrontApp, Inc., a company incorporated in Delaware, and its worldwide affiliates and subsidiaries (collectively, "**Front**"), and the entity identified below ("**Customer**"). Front and Customer may each be referred to as a "**Party**" and collectively referred to as the "**Parties**". This DPA shall be effective on the date it has been fully executed by the Parties and if it has been provided to Front in accordance with the instructions below (the "**DPA Effective Date**"). As of the DPA Effective Date, this DPA shall be incorporated by reference into the agreement between Customer and Front that governs Customer's use of the Service, whether such agreement is online or in a written agreement executed in counterparts with Front ("**Agreement**"). All capitalized terms used in this DPA but not defined shall have the meaning set forth in the Agreement. To the extent of any conflict or inconsistency between this DPA and the remaining terms of the Agreement, this DPA will govern. This DPA replaces in its entirety any previously applicable data processing agreement entered into or agreed upon by the parties prior to the DPA Effective Date.

This DPA sets out the terms that apply when Personal Data is Processed by Front under the Agreement. The purpose of the DPA is to ensure such Processing is conducted in accordance with Applicable Law and respects the rights of individuals whose Personal Data are Processed under the Agreement.

HOW TO EXECUTE THIS DPA

This DPA and the Standard Contractual Clauses attached as Exhibit A have been pre-signed by Front. When Front receives the completed and signed DPA and Standard Contractual Clauses as specified below, this DPA and the Standard Contractual Clauses will become a legally binding addendum to the Agreement. To make this DPA and the Standard Contractual Clauses a part of the Agreement, Customer must:

1. Complete the information in the signature blocks on page 5 of this DPA.
2. Complete the information as Data Exporter on Page 8.
3. Submit the completed and signed DPA and the completed Standard Contractual Clauses via email to compliance@frontapp.com.

1. Definitions

"**Applicable Law(s)**" means all applicable laws, regulations, and other legal or regulatory requirements in any jurisdiction relating to privacy, data protection/security, or the Processing of Personal Data, including without limitation the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.* ("**CCPA**") and the General Data Protection Regulation, Regulation (EU) 2016/679 ("**GDPR**"). For the avoidance of doubt, if Front's processing activities involving Personal Data are not within the scope of an Applicable Law, such law is not applicable for purposes of this Addendum.

"**EEA**" means the European Economic Area, which constitutes the member states of the European Union and Norway, Iceland and Liechtenstein, as well as, for the purposes of this DPA, Switzerland and the United Kingdom.

"**Personal Data Breach**" means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

"**Personal Data**" means any Customer Content that includes "personal data," "personal information," and "personally identifiable information," and such terms shall have the same meaning as defined by Applicable Law.

"**Process**" and "**Processing**" mean any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission,

dissemination or otherwise making such data available, alignment or combination, restriction, erasure or destruction.

"**Standard Contractual Clauses**" means the agreement by and between Front and Customer, attached hereto as Exhibit A, pursuant to the EU Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of Personal Data from the EEA to processors established in third countries under Directive 95/46/EC of the European Parliament and of the European Council, completed as described in the "Data Transfers" section below.

"**Subprocessor**" means any Front affiliate or party engaged by Front for the Processing of Personal Data in connection with the Service.

2. Relationship of the Parties

Customer is (or represents that it is acting with full authority on behalf of) the "**Controller**", and Front is the "**Processor**", as such terms (or the equivalent thereof) are defined in Applicable Law, with respect to the Personal Data Processed under the Agreement. In some circumstances, Customer may be a Processor, in which case Customer appoints Front as Customer's subprocessor, which shall not change the obligations of either Customer or Front under this DPA.

3. Customer's Instructions to Front

3.1 Purpose Limitation. Front will not sell Personal Data or otherwise Process Personal Data for any purpose other than for the specific purposes set forth in this DPA or the Agreement, unless obligated to do otherwise by Applicable Law. In such case, Front will inform Customer of that legal requirement before the Processing unless legally prohibited from doing so. Further details regarding Front's Processing operations are set forth in Exhibit B. For purposes of this paragraph, "sell" shall have the meaning set forth in the CCPA.

3.2 Lawful Instructions. Customer will not instruct Front to Process Personal Data in violation of Applicable Law. Front has no obligation to monitor the compliance of Customer's use of the Service with Applicable Law. Front will immediately inform Customer if, in Front's opinion, an instruction from Customer infringes Applicable Law. The Agreement, including this DPA, along with Customer's configuration of the Service (as Customer may be able to modify from time to time) and any features applicable to Customer's then-current version of the Service, constitute Customer's complete and final instructions to Front regarding the Processing of Personal Data, including for purposes of the Standard Contractual Clauses.

4. Subprocessing

4.1 Appointment of Subprocessors; List; Liability. Customer acknowledges and agrees that Front may retain certain third parties as Subprocessors to Process Personal Data on Front's behalf (under this DPA as well as under the Standard Contractual Clauses, if applicable) in order to provide the Service. A list of Front's third-party Subprocessors, which may be updated from time to time, is maintained at https://frontapp.com/list-of-subprocessors. Prior to a Subprocessor's Processing of Personal Data, Front will impose contractual obligations on the Subprocessor substantially the same as those imposed on Front under this DPA. Front remains liable for its Subprocessors' performance under this DPA to the same extent Front is liable for its own performance.

4.2 Objection Right for New Subprocessors. Customer may reasonably object to Front's use of a new Subprocessor (e.g., if making Personal Data available to the Subprocessor may violate Applicable Laws or weaken the protections for such Personal Data) by notifying Front in writing. Customer's notice shall explain in reasonable detail Customer's grounds for a good-faith objection. If Front is

unable to satisfactorily address Customer's objection, within a reasonable period of time not to exceed 60 days, then either party may terminate the Agreement upon written notice. In the event of such termination, Front will refund to Customer any prepaid but unused fees, as calculated on a pro-rata basis.

4.3 Copies of Subprocessor Agreements Pursuant to the Standard Contractual Clauses. The parties agree that copies of the Subprocessor agreements that must be provided to Customer pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, redacted by Front and that such copies will be provided by Front only upon written request of Customer and in a manner determined by Front.

5. Assistance & Cooperation

5.1 Security. Front will provide reasonable assistance to Customer regarding Customer's compliance with its security obligations under Applicable Law relevant to Front's role in Processing the Personal Data, taking into account the nature of Processing and the information available to Front, by implementing technical and organizational measures set forth in the Agreement, without prejudice to Front's right to make future replacements or updates to the measures that do not lower the level of protection of Personal Data. Front will ensure that the persons Front authorizes to Process the Personal Data are subject to written confidentiality agreements or are under an appropriate statutory obligation of confidentiality no less protective than the confidentiality obligations set forth in the Agreement.

5.2 Personal Data Breach Notification & Response. Front will comply with the Personal Data Breach-related obligations directly applicable to it under Applicable Law. Taking into account the nature of Processing and the information available to Front, Front will assist Customer by informing it of a confirmed Personal Data Breach without undue delay or within the time period required under Applicable Law. Front will notify Customer at the email address provided in the signature block of this DPA for purposes of Personal Data Breach notifications. Any such notification is not an acknowledgement of fault or responsibility. To the extent available, this notification will include Front's then-current assessment of the following, which may be based on incomplete information:

(a) the nature of the Personal Data Breach, including, where possible, the categories and approximate number of data subjects concerned;

(b) the likely consequences of the Personal Data Breach; and

(c) measures taken or proposed to be taken by Front to address the Personal Data Breach, including, where applicable, measures to mitigate its possible adverse effects.

Front will not assess the contents of Customer Data in order to identify information subject to any specific legal requirements. Customer is solely responsible for complying with legal requirements for incident notification applicable to Customer and fulfilling any third-party notification obligations related to any Customer Data Incident(s). Nothing in this DPA or in the Standard Contractual Clauses shall be construed to require Front to violate, or delay compliance with, any legal obligation it may have with respect to a Personal Data Breach or other security incidents generally.

6. Responding to Individuals Exercising Their Rights Under Applicable Law

To the extent legally permitted, Front shall promptly notify Customer if Front receives any requests from an individual seeking to exercise any rights afforded to them under Applicable Law regarding their Personal Data, which may include: access, rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, objection to the Processing, or to not be subject to an automated individual decision making (each, a "**Data Subject Request**"). Customer may request in writing that Front use commercially reasonable efforts to assist Customer in addressing a Data Subject Request. Front shall assist Customer to the extent legally permitted to do so and if response to such Data Subject Request is required under Applicable Law. To the extent legally permitted, Customer shall be responsible for any costs arising from Front's provision of such assistance, including any fees associated with provision of additional functionality.

7. DPIAs and Consultation with Supervisory Authorities or other Regulatory Authorities

Taking into account the nature of the Processing and the information available to Front, Front will provide reasonable assistance to Customer's performance of any legally required data protection impact assessment of the Processing or proposed Processing of the Personal Data involving Front. Front may provide such assistance, in consultation with supervisory authorities or other regulatory authorities as required, by providing Customer with any publicly available documentation for the Service or by complying with the Audits section below. Additional support for data protection impact assessments or relations with regulators may be available and would require mutual agreement on fees, the scope of Front's involvement, and any other terms that the Parties deem appropriate.

8. Data Transfers

8.1 Customer authorizes Front and its Subprocessors to make international transfers of the Personal Data in accordance with this DPA so long as Applicable Law for such transfers is respected. As of the DPA Effective Date, Front is a member of the EU-U.S. and Swiss-U.S. Privacy Shield frameworks (each a "**Privacy Shield Certification**").

8.2 For transfers of Personal Data subject to Applicable Law under this DPA from (a) the EEA to (b) countries which do not ensure an adequate level of data protection within the meaning of Applicable Law:

(a) Front's Privacy Shield Certifications (as applicable) shall apply; provided

(b) To the extent any Privacy Shield Certification is invalidated, or Front's participation in any such Privacy Shield Certification lapses, then the Standard Contractual Clauses attached hereto as Exhibit A shall apply; provided, further

(c) Front may provide Customer with written notice if it becomes certified under an alternative transfer of Personal Data framework approved by relevant authorities. Upon such written notice, such alternative framework will supersede the Standard Contractual Clauses.

9. Audits

If and to the extent required by Applicable Law, Front shall assist with audits of Front, including inspections, conducted by Customer or another third-party representative mandated by Customer. Any such audits shall be subject to the following conditions: so long as the Agreement remains in effect and at Customer's sole expense, Customer may request that Front provide it with documentation, data, and records ("**Records**") no more than once annually relating to Front's compliance with this DPA (an "**Audit**"). To the extent Customer uses a third-party representative to conduct the Audit, Customer shall ensure that such third-party representative is bound by

obligations of confidentiality no less protective than those contained in this Agreement. Customer shall provide Front with fifteen (15) days prior written notice of its intention to conduct an Audit. Customer shall conduct its Audit in a manner that will result in minimal disruption to Front's business operations. Customer shall not be entitled to receive data or information of other clients of Front or any other Front Confidential Information not directly relevant for the authorized purposes of the Audit. If any material non-compliance is identified by an Audit, Front shall take prompt action to correct such non-compliance. For the avoidance of doubt, this provision does not grant Customer any right to conduct an on-site audit of Front's premises. Front reserves the right to require Customer to reimburse Front for time expended for an Audit at Front's then-current rates, which shall be made available to Customer upon request. The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with this Section.

10. Return or Destruction of Personal Data

Upon written request from Customer's authorized representative (which for purposes of this section is any Customer employee (a) that is either a billing owner or an Administrator of the Service, or (b) who has confirmed in writing that they are authorized to make decisions on behalf of the Customer), Front shall delete or anonymize such Personal Data in accordance with its requirements under Applicable Law. Notwithstanding the foregoing, this provision will not require Front to delete Personal Data from archival and back-up files except as provided by Front's internal data deletion practices and as required by Applicable Law.

[*Signature Page to follow*]

Accepted and agreed to by the authorized representatives of each Party:

FrontApp, Inc.	Customer: _____
By: Stephanie Hu	By:
Name: Stephanie Hu	Name:
Title: Head of Legal	Title:
Date: August 24, 2020	Date:
Address: 1455 Market Street, 19th Floor San Francisco, CA 94103 Attn: Legal Department	Address: _____ _____ _____
Notice Copy: compliance@frontapp.com	Email Address:
	Data Protection Officer (if any):
	GDPR Representative in the EEA (if any):

Exhibit A

Standard Contractual Clauses

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 data exporting organization (the "**Data Exporter"**): _____

Address: _____
_____
_____

Email: _____

and

FrontApp, Inc. (the **"Data Importer"**)

Address: 1455 Market Street, 19th Floor
San Francisco, CA 94103
_____

Email: compliance@frontapp.com

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.

Clause 1

Definitions

For the purposes of the Clauses, the Definitions are outlined above.

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, and from 25 May 2018 within the meaning of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation);

(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 documented instructions and the Clauses; and it shall not disclose personal data transferred to third parties (including for back-up purposes) apart from subprocessors authorised by the Data Exporter under this Agreement. If the Data Importer 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 and/or take any other reasonable action;

(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 non-compliance by the Data Importer or its employees with this Agreement or the regulatory provisions relating to the protection of transferred personal data processed under this Agreement;

(ii) 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;

(iii) any accidental or unauthorised access;

(iv) any notice, inquiry or investigation by a supervisory authority; and

(iv) 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;

(k) in discharging its obligations under this Agreement, to be responsible for its compliance with applicable data protection law and will ensure that all necessary registrations and notifications are made and provide the Data Export with a copy, on request, of evidence of such and evidence of any amendments or alterations made thereto;

(l) to send promptly a copy of any subprocessor agreement, authorised by the Data Exporter, that the Data Importer concludes under the Clauses to the Data Exporter;

(m) to take all reasonable steps to ensure that (i) persons employed by it, and (ii) other persons engaged at its place of business, who will process transferred personal data, are aware of and comply with this Agreement;

(n) to comply with strict confidentiality obligations in respect of transferred personal data and ensure that its employees, authorised agents and any subprocessors are legally required in writing to comply with and respect the confidentiality of the transferred personal data, including at the end of their employment, contract or at the end of their assignment;

(o) to deal promptly, properly and in good faith with all reasonable inquiries relating to the Data Importer's processing of transferred personal data whether such inquiry is made by the Data Exporter, a data subject or any supervisory authority;

(p) to fully co-operate with and assist the Data Exporter, without delay in respect of its obligations regarding:

(i) requests from data subjects in respect of access to or the rectification, erasure, restriction, blocking or deletion of transferred personal data. In the event that the data subject sends such a request directly to the Data Importer, they will pass it on to the Data Exporter without delay;

(ii) the investigation of any accidental or unauthorised access and any notification to a supervisory authority and data subjects in respect of such accidental or unauthorised access;

(iii) the preparation of data protection impact assessments and, where applicable, carrying out consultations with a supervisory authority;

(iv) the security of transferred data, including by implementing the technical and organizational security measures

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 Clauses.

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.

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer): Customer, a user of the Service.

Data importer

The data importer is (please specify briefly activities relevant to the transfer): FrontApp, Inc. and its worldwide affiliates and subsidiaries (collectively, "Front"), provider of the Service.

Data subjects

The Personal Data transferred concern the following categories of data subjects (please specify): Depending on Customer's usage, this could include the data exporter's personnel, as well as individuals in other categories, such as the data exporter's customers, service providers, business partners, affiliates and other End Users.

Categories of Personal Data

The Personal Data transferred concern the following categories of data (please specify): The Service does not impose a technical restriction on the categories of Personal Data Customer may provide. The Personal Data Processed by Front may thus include name, email address, telephone, title, and other categories of Personal Data, subject to the following section.

Special categories of data (if appropriate)

Customer may submit personal data to Front through the Service, the extent of which is determined and controlled by Customer in compliance with Applicable Laws and which may concern the following special categories of data, if any: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade-union membership; genetic or biometric data; sex life or sexual orientation; and physical or mental health or condition.

Processing operations

The Personal Data transferred will be processed in accordance with the Agreement and may be subject to the following processing activities: storage and other processing necessary to provide, maintain and update the Service; provide customer and technical support to Customer; and disclosures in accordance with the Agreement, as required by law.

Duration of Processing

The Personal Data will be Processed for the duration of the Agreement, subject to Section 10 of this DPA.

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses.

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) can be found in the Agreement between the Parties.

Exhibit B

Front Processing Operations

Data subjects

The Personal Data transferred concern the following categories of data subjects (please specify): Depending on Customer's usage, this could include the data exporter's personnel, as well as individuals in other categories, such as the data exporter's customers, service providers, business partners, affiliates and other End Users.

Categories of Personal Data

The Personal Data transferred concern the following categories of data (please specify): The Service does not impose a technical restriction on the categories of Personal Data Customer may provide. The Personal Data Processed by Front may thus include name, email address, telephone, title, and other categories of Personal Data, subject to the following section.

Customer may submit personal data to Front through the Service, the extent of which is determined and controlled by Customer in compliance with Applicable Laws and which may concern the following special categories of data, if any: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade-union membership; genetic or biometric data; sex life or sexual orientation; and physical or mental health or condition.

Processing operations

The Personal Data transferred will be processed in accordance with the Agreement and may be subject to the following processing activities: storage and other processing necessary to provide, maintain and update the Service; provide customer and technical support to Customer; and disclosures in accordance with the Agreement, as required by law.