

## 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 Data Protection Law and respects the rights of individuals whose Personal Data are Processed under the Agreement.

### HOW TO EXECUTE THIS DPA

This DPA has been pre-signed by Front and being provided to Customer for electronic signature. When Front receives the completed and signed DPA via our electronic signature platform, this DPA, including all Schedules will become a legally binding addendum to the Agreement. To make this DPA a part of the Agreement, Customer must:

1. Use our electronic signature platform to complete the information in all of the signature blocks as indicated below.
2. Submit the completed and signed DPA via our electronic signature platform.
3. Customer will receive a fully signed copy of this DPA for its records upon proper completion using our electronic signature platform.

### 1. Definitions

“**Account Administration Data**” means Personal Data contained in customer information used by Front for account administration and in connection with establishing and maintaining Front’s business relationship with Customer. Account Administration Data does not include Customer Data.

“**Applicable Data Protection 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.*, and its implementing regulations (“CCPA”), the General Data Protection Regulation, Regulation (EU) 2016/679 (“GDPR”), and the UK General Data Protection Regulation and any other corresponding laws of the United Kingdom. For the avoidance of doubt, if Front’s processing activities involving Personal Data are not within the scope of an Applicable Data Protection Law, such law is not applicable for purposes of this DPA.

“**Customer Data**” means Personal Data contained in Customer Content. Customer Data does not include Account Administration Data.

“**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.

“**Personal Data**” means “personal data,” “personal information,” “personally identifiable information,” or similar information as defined by Applicable Data Protection Law.

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

“**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.

“**Sub-processor**” means any party engaged by Front for the Processing of Customer Data in connection with the Service.

## 2. Relationship of the Parties

- 2.1 Front as Processor. Customer is the “**Controller**”, and Front is the “**Processor**”, as such terms (or the equivalent thereof) are defined in Applicable Data Protection Law, with respect to the Customer Data Processed under the Agreement.
- 2.2 Front as Controller. Customer and Front are each “**Controllers**”, as such term (or the equivalent thereof) is defined in Applicable Data Protection Law, with respect to Account Administration Data, and Front will Process such data in accordance with the Agreement, Front’s Privacy Policy available at <https://front.com/privacy-policy> as may be updated from time to time, and Applicable Data Protection Laws.

## 3. Customer’s Instructions to Front

- 3.1 Purpose Limitation. Front will not sell Customer Data or otherwise Process Customer 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 Data Protection 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 Schedule 1 - Subject Matter & Details of Processing. 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 Customer Data in violation of Applicable Data Protection Law. Front has no obligation to monitor the compliance of Customer’s use of the Service with Applicable Data Protection Law. Front will immediately inform Customer if, in Front’s opinion, an instruction from Customer infringes Applicable Data Protection Law. The Agreement, Customer’s configuration of the Service, and this DPA constitute Customer’s instructions to Front regarding the Processing of Customer Data. Customer instructs Front to process Customer Data to provide the Services and authorizes Front to Process such data to (a) perform its obligations and exercise its rights under the Agreement, and (b) to perform its legal obligations and to establish, exercise or defend legal claims in respect of the Agreement.

## 4. Sub-processing

- 4.1 Appointment of Sub-processors. Customer acknowledges and agrees that (a) Front’s Affiliates may be retained as Sub-processors; and (b) Front and Front’s Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. Front or an Front Affiliate has entered into a written agreement with each Sub-processor containing, in substance, data protection obligations no less protective than those in the Agreement with respect to the protection of Customer Data to the extent applicable to the nature of the Services provided by such Sub-processor.
- 4.2 List of Current Sub-processors and Notification of New Sub-processors. The current list of Sub-processors engaged in Processing Personal Data for the performance of each applicable Service, including a description

of their processing activities and countries of location can be found on Front's webpage at: <https://frontapp.com/list-of-subprocessors>. Customer hereby consents to these Sub-processors, their locations and processing activities as it pertains to their Personal Data. The webpage contains a mechanism to subscribe to notifications of new Sub-processors; and, if Customer subscribes, Front shall provide notification of a new Sub-processor(s) before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services.

- 4.3 Objection Right for New Sub-processors. Customer may object to Front's use of a new Sub-processor by notifying Front promptly in writing within thirty (30) days of receipt of Front's notice in accordance with the mechanism set out in section 4.2. If Customer objects to a new Sub-processor as permitted in the preceding sentence, Front will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Front is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Customer may terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by Front without the use of the objected-to new Sub-processor by providing written notice to Front. Front will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.
- 4.4 Liability. Front shall be liable for the acts and omissions of its Sub-processors to the same extent Front would be liable if performing the services of each Sub-processor directly under the terms of this DPA, unless otherwise set forth in the Agreement.

## 5. Assistance & Cooperation

- 5.1 Security. Front will provide reasonable assistance to Customer regarding Customer's compliance with its security obligations under Applicable Data Protection Law relevant to Front's role in Processing the Customer Data, taking into account the nature of Processing and the information available to Front, by implementing technical and organizational measures set forth in Schedule 2 - Technical and Organizational Security Measures, without prejudice to Front's right to make future replacements or updates to the measures that do not lower the level of protection of Customer Data. Front will ensure that its personnel authorized to Process the Customer 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 Data Protection 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 Data Protection Law unless prohibited by 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.

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 incidents involving Customer Data. Nothing in this DPA, including the Schedules and any Standard Contractual Clauses referenced therein, 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 Data Protection 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 Data Protection Law related to Customer 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 Data Protection 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 Customer 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 (including Front's affiliates) and its Sub-processors to make international transfers and onward transfers of Personal Data in accordance with this DPA and as set forth in Schedule 3 - International Personal Data Transfers so long as Applicable Data Protection Law for such transfers is respected.
- 8.2 Front will comply with the principals set forth in the EU-U.S. and Swiss-U.S. Privacy Shield Framework. Notwithstanding Schedule 3 - International Data Transfers, if Front adopts an alternate data transfer mechanism permitted or approved under Applicable Data Protection Laws that covers the transfer of Personal Data to a third country, then such transfer mechanism shall govern the transfer of Personal Data.

## **9. Audits**

If and to the extent required by Applicable Data Protection Law, Front shall assist with audits concerning Front's compliance with this DPA as it relates to Front's Processing of Customer Data. 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 as relates to Front's Processing of Customer Data (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 and

Customer shall be fully liable to Front for any breaches of confidentiality by its third-party representatives. 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. This provision does not grant Customer any right to conduct an on-site audit of Front's premises unless mandated by Applicable Data Protection Law. 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. Customer agrees that any audit rights granted by Applicable Data Protection Laws will be satisfied by this Section 9.

#### **10. Return or Destruction of Customer Data**

Upon written request to delete Customer Data 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 Customer Data in accordance with its requirements under Applicable Data Protection Law. Notwithstanding the foregoing, (i) this provision will not require Front to delete Customer Data from archival and back-up files except as provided by Front's internal data deletion practices and as required by Applicable Data Protection Law and (ii) Front may retain Customer Data if permitted by applicable law, provided such data will remain subject to the requirements of this Addendum.

#### **11. Limitations on Liability**


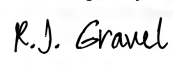
Any liabilities arising under this DPA are subject to the limitations of liability and indemnification provisions in the Agreement.

#### **12. Governing Law**

This DPA will be governed and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless otherwise required by Applicable Data Protection Law.

*[Signature Page to follow]*

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

FrontApp, Inc.	Customer Entity Name: <u>Glenbrook HSD 225</u>
By: 	By: 
Name: Jason Robman	Name: <small>A0C627368AC945D...</small> R.J. Gravel
Title: Head of Legal	Title: Associate Superintendent
	Date: 4/4/2022
Address: 1455 Market Street, 19 <sup>th</sup> Floor San Francisco, CA 94103 Attn: Legal Department	Address: 3801 W. Lake Avenue, Glenview, IL _____ _____
Notice Copy: privacy@frontapp.com	Email Address for Notices: rgrave1@glenbrook225.org
	Data Protection Officer (if any): n/a
	GDPR Representative in the EEA (if any):

**SCHEDULE 1**  
**Subject Matter & Details of Processing**

**Categories of Data Subjects**

**Customer Data:**

Except in connection with the use and content guidelines set forth or referenced in the Agreement, Front's Services do not impose any limits on the categories of data subjects. The data subjects are determined and controlled by Customer in its sole discretion, and may include, but are not limited to Customer's personnel, as well as individuals in other categories, such as the customers, service providers, business partners, affiliates and other End Users of Customer.

**Account Administration Data:**

The data subjects include Customer's employees, contractors, and consultants.

**Categories of Personal Data**

**Customer Data:**

Except in connection with the use and content guidelines set forth or referenced in the Agreement, Front's Services do not impose any limits on the categories of Personal Data stored, transferred or otherwise Processed. The types of Personal Data are determined and controlled by Customer in its sole discretion, and may include, but are not limited to name, email address, address, telephone number, title, and any other Personal Data included in Customer Content.

**Account Administration Data:**

The Personal Data Processed and/or transferred include name, email address, telephone, title, IP address, and address.

**Sensitive Data or Special Categories of Data**

**Customer Data:**

Customer may submit Personal Data to Front through the Service, the extent of which and legal basis for processing are determined and controlled by Customer. Personal Data 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.

**Account Administration Data:**

None.

**Processing operations/Nature and purpose of the Transfer and other Processing**

**Customer Data:**

Front will Process and/or transfer Customer Data in accordance with the Agreement and as necessary to provide the Services under the Agreement. Customer Data 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. Front will process Customer Data in accordance with and for the purposes of complying with Customer's instructions as set forth in Section 3.2 of this DPA.

**Account Administration Data:**

Front will Process and/or transfer Account Administration Data in accordance with the Agreement and Front's Privacy Policy available at <https://front.com/privacy-policy>, as may be updated from time to time. The Processing and/or transfer is primarily to administer and troubleshoot Customer's account and in connection with establishing and maintaining Front's business relationship with Customer.

**Duration of Processing/Period for which Personal Data will be retained**

The duration of the processing of Customer Data under this DPA is determined by Customer.



## **SCHEDULE 2**

### **Technical and Organizational Security Measures**

#### ***Measures of pseudonymisation and encryption of personal data***

Data is encrypted both in transit and at rest. In transit, Front uses TLS 1.2 or greater for data encryption between Front and third parties, including customers. At rest, Front leverages its hosting subprocessor, Amazon Web Services (AWS) to store data, which allows for data to be encrypted at rest using RDS, EBS, and S3.

Amazon Relational Database Service (RDS) encrypts databases using keys that are managed using Front's Amazon Key Management System (KMS). RDS encryption uses the industry standard AES-256 encryption algorithm to encrypt your data on the server that hosts your RDS instance.

#### ***Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services***

Front ensures strict confidentiality through encryption of customer data, identity and access (both logical and physical) management.

Integrity is maintained by requiring all code changes to undergo a second code review before deploying to production. Access to data is restricted and logged to prevent unauthorized data modification and corruption.

Front infrastructure runs on AWS and is spread across several AWS Availability Zones. Front has a scalable architecture, with a number of parameters that can autoscale based on demand.

#### ***Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident***

Front performs daily backups using an automated system in AWS. Datastores are retained for 10 days. Backup data is also stored in a separate AWS availability zone allowing recovery in the event of a physical or technical incident.

Front maintains a disaster recovery plan to allow for orderly and effective recovery. The plan is tested on an annual basis.

#### ***Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing***

Front undergoes an annual third-party penetration testing. In addition, Front undergoes an annual SOC 2 Type II audit performed by an independent third-party auditor to assess the suitability of the design and effectiveness of our controls.

#### ***Measures for user identification and authorisation***

Front allows customers to enable multi-factor authentication. Front maintains a principle of least privilege on its business systems and all uses of elevated privilege are logged. Front requires all production systems to be accessed only via VPN secured with multi-factor authentication.

#### ***Measures for the protection of data during transmission***

Please see "Measures of pseudonymisation and encryption of personal data" above.

#### ***Measures for the protection of data during storage***

Please see "Measures of pseudonymisation and encryption of personal data" above.

***Measures for ensuring physical security of locations at which personal data are processed***

Personal data is processed by our hosting subprocessor, Amazon Web Services (AWS). AWS data center facilities are ISO 27001:2013 certified and undergo periodic SOC 1 and SOC 2 Type 2 report audits. Certification status and the results of audits are reviewed periodically as part of Front monitoring controls and the vendor management process. Physical access to Front's offices is strictly controlled with keycards and security guards at the building entrances.

***Measures for ensuring events logging***

System logging and monitoring software is used to collect data from system infrastructure components and endpoints, to monitor for potential security threats and vulnerabilities, and to detect unusual system activity or service requests. Front enables alerting when credentials for certain privileged systems are used.

***Measures for ensuring system configuration, including default configuration***

Infrastructure is virtualized with AWS. Our cloud infrastructure is deployed from Terraform templates. Changes to the system configuration and infrastructure must undergo peer review to guard against unauthorized changes.

***Measures for internal IT and IT security governance and management***

Front has an Information Security Management System (ISMS) committee that is responsible for security and compliance efforts internally. The ISMS committee meets quarterly to review strategic initiatives, assess key risk and threats to the company, and track progress on the remediation of risks identified during the annual internal risk assessment and third party penetration test.

The ISMS committee exercises oversight of security controls by reviewing the ISMS policy on an annual basis. In addition, the ISMS committee communicates security and compliance efforts to Front's board of directors on a quarterly basis.

***Measures for certification/assurance of processes and products***

Front performs annual third-party penetration testing and has SOC 2 Type II attestation. Front has developed an Information Security Management System (ISMS) based on ISO27001 standards.

***Measures for ensuring data minimisation***

Front collects data for the delivery of service and to facilitate third party subprocessor service if needed. Front will inform the user at the point of data collection if certain data must be provided.

***Measures for ensuring data quality***

Front leverage testing and input validation to ensure the quality of data entering our systems is complete. Users can correct or complete data they deemed to be inaccurate or incomplete. Front implements access controls and logging for data systems to prevent possible data corruption.

***Measures for ensuring limited data retention***

Upon written request, customers can request their data to be deleted within the timeline specified in the Data Protection Addendum and in accordance with Applicable Data Protection Law.

***Measures for ensuring accountability***

Front conducts regular third-party audits to ensure compliance with our privacy and security standards.

***Measures for allowing data portability and ensuring erasure***

Front allows users the right to obtain personal data in a structured, commonly used and machine-readable format. Users can ask Front to delete or remove their data and such requests will be processed within 30 days.

**SCHEDULE 3**  
**International Personal Data Transfers**

**1. EEA Data Transfers:**

- (a) *Customer Data Transfers Within the EEA:* Customers with a principal place of business located in the EEA or who elect to have Customer Data stored in the EEA (each, “**EEA Customers**”) will most commonly transfer Customer Data to Front within the EEA. In this case, Front is the Data Exporter. Customer authorizes Front to transfer Personal Data outside of the EEA to (i) Front’s affiliates, (ii) Front’s contractors and consultants outside the EEA, and (iii) Front’s Sub-processors; provided that Front will enter into Module Three of the Standard Contractual Clauses approved by the European Commission (Processor to Processor) in decision 2021/914 currently available at [https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en) (the “**EU SCCs**”) with any such Sub-processors, or (ii) ensures another transfer mechanism permitted under Applicable Data Protection Law is in place. Customer authorizes Front, Front’s affiliates and its Sub-processors to transfer Customer Data to the third parties listed at <https://frontapp.com/list-of-subprocessors>, including third parties listed on any Sub-processor pages listed therein.
- (b) *Customer Data Transfers Outside the EEA:* (i) Customers with a principal place of business located outside the EEA but Customer Data in the EEA will most commonly transfer Customer Data from within the EEA to Front as Customer’s Processor outside the EEA. (ii) EEA Customers may transfer data outside the EEA in limited circumstances. In the event of (i) or (ii), if required by Applicable Data Protection Law, each Party agrees to abide by and transfer Customer Data in accordance with Module Two of the EU SCCs, which are incorporated into this DPA by reference. Each party is deemed to have executed Module 2 of the EU SCCs by entering into this DPA, and the following shall apply:

- in Clause 9(a), the Parties choose Option 2, and the time period to notify Customer of changes to sub-processors is at least seven days in advance;
- in Clause 11(a), the optional language will not apply;
- in Clause 17, the Parties choose Option 1, and the governing law is Ireland;
- in Clause 18(b), the forum will be Ireland;
- in Annex I, Part A:

Data Exporter: Customer

Address and Other Contact Details: As set forth in the signature block on page 6 of the DPA.

Data Exporter Role: Controller of Customer Data.

Signature and Date: Customer’s execution of the DPA is deemed a signature of the applicable Standard Contractual Clauses included herein, including their Annexes, as of the effective date of the DPA.

Activities relevant to the data transferred are set forth in Schedule 1.

Data Importer: FrontApp, Inc.

Address and Other Contact Details: [compliance@frontapp.com](mailto:compliance@frontapp.com)

Data Importer Role: Processor of Customer Data.

Signature and Date: Front’s execution of the DPA is deemed a signature of the applicable Standard Contractual Clauses included herein, including their Annexes, as of the effective date of the DPA.

Activities relevant to the data transferred are set forth in Schedule 1;

- In Annex I, Part B

Schedule 1 sets forth the categories of data subjects, categories of Personal Data transferred, sensitive data transferred, nature of the processing, purpose of the data transfer and further processing, and period of the processing.

The frequency of the transfer is continuous.

For transfers to Sub-processors, the subject matter, nature and duration of the processing is outlined at <https://frontapp.com/list-of-subprocessors>;

- In Annex I, Part C

The competent supervisory authority is Ireland Data Protection Commission; and

- In Annex II:

Schedule 2 sets forth Front's technical and organizational measures.

## 1.2 Account Administration Data

(a) *Account Administration Data Transfers Outside the EEA*: When Customer transfers Account Administration Data from within the EEA to Front as a Controller outside the EEA, each Party agrees to abide by and transfer Account Administration Data in accordance with Module One of the EU SCCs, which are incorporated into this DPA by reference. Each party is deemed to have executed the EU SCCs by entering into this DPA, and the following shall apply:

- in Clause 11(a), the optional language will not apply;
- in Clause 17, the Parties choose Option 1, and the governing law is Ireland;
- in Clause 18(b), the forum will be Ireland;
- in Annex I, Part A:

Data Exporter: Customer

Address and Other Contact Details: As set forth in the signature block on page 6 of the DPA.

Data Exporter Role: Controller of Account Administration Data.

Signature and Date: Customer's execution of the DPA is deemed a signature of the applicable Standard Contractual Clauses included herein, including their Annexes, as of the effective date of the DPA.

Activities relevant to the data transferred are set forth in Schedule 1.

Data Importer: FrontApp, Inc.

Address and Other Contact Details: [compliance@frontapp.com](mailto:compliance@frontapp.com).

Data Importer Role: Controller of Account Administration Data.

Signature and Date: Front's execution of the DPA is deemed a signature of the applicable Standard Contractual Clauses included herein, including their Annexes, as of the effective date of the DPA.

Activities relevant to the data transferred are set forth in Schedule 1;

- In Annex I, Part B

Schedule 1 sets forth the categories of data subjects, categories of Personal Data transferred, sensitive data transferred, nature of the processing, purpose of the data transfer and further processing, and period of the processing.

The frequency of the transfer is continuous.

For transfers to Sub-processors, the subject matter, nature and duration of the processing is outlined at <https://frontapp.com/list-of-subprocessors>;

- In Annex I, Part C

The competent supervisory authority is Ireland Data Protection Commission; and

- In Annex II:

Schedule 2 sets forth Front's technical and organizational measures.

2. **UK Data Transfers:** For transfers of Personal Data subject to Applicable Data Protection Law under the DPA from (a) the United Kingdom to (b) countries which do not ensure an adequate level of data protection within the meaning of Applicable Data Protection Law, the following terms shall govern:

- 2.1 The Standard Contractual Clauses (Processors) approved by the European Commission in decision 2010/87 available at <https://op.europa.eu/en/publication-detail/-/publication/473b885b-31d6-4f3b-a10f-01152e62be6e/language-en> shall apply to applicable transfers of Customer Data. Customer will be and will comply with the obligations of the data exporter, Front will be and will comply with the obligations of the data importer. The information required for Appendix 1 is set out in Schedule 1, and the information required for Appendix 2 is set out in Schedule 2.

The parties agree that copies of the Sub-processor 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.

- 2.2 The Standard Contractual Clauses (controller to controller transfers) Set II approved by the European Commission in decision 2004/915 available at <https://op.europa.eu/en/publication-detail/-/publication/57a11830-3866-44bf-a03a-0384f7b3d3d6/language-en> shall apply to applicable transfers of Account Administration Data. Customer will be, and will comply with the obligations of the data exporter, Front will be and will comply with the obligations of the data importer and, for the purposes of Clause II(h), will comply with the data processing principles set forth in Annex A. The information required for Annex B is set out in Schedule 1.