



## MASTER SAAS AND SERVICES AGREEMENT

**THIS MASTER SAAS AND SERVICES AGREEMENT** (the “**Services Agreement**”) is made this day of October 19, 2022 the “**Effective Date**”,

By and Between:

Hard Rock Cafe International (USA), Inc. whose mailing address/registered office is at \_\_\_\_\_ (“**Parent**”) on behalf of itself and Parent’s Affiliates which are Customers

And

**Frontline Performance Group, LLC** (hereinafter called the “**Company**” or “**FPG**”) whose mailing address/registered office is at 1075 West Morse Boulevard, Winter Park, Florida USA 32789

(The Company, the Parent and the Customers collectively referred to as the “**Parties**” and each a “**Party**”)

**WHEREAS**, Company provides certain Services on a subscription basis and related Professional Services;

**WHEREAS**, Parent has approved the sale of such Services by FPG to Parent branded hotels and hotels managed by Parent’s Affiliates (each known as a “**Customer**”); and

**WHEREAS**, those Parent branded hotels and hotels managed by Parent’s Affiliates choosing to subscribe to such Services, will do so directly with the Company pursuant to the terms of a Work Order.

**NOW, THEREFORE**, in consideration of the mutual promises contained in this Agreement, Company and Parent agree to the following terms and conditions.

### 1. General

- 1.1. Incorporation of GTC. Parent, on behalf of itself and the Customers accepts FPG’s General Terms and Conditions (“**GTC**”) to enable the delivery of the subscribed Services contemplated in this Services Agreement. Parent, on behalf of itself and the Customers, hereby agrees that the terms and provisions of the GTC are hereby fully incorporated into this Services Agreement by this reference.
- 1.2. Terms and Interpretation. Unless otherwise defined in this Services Agreement, capitalized terms will have the meaning set forth in the GTC. Terms, acronyms and phrases known in the information technology industry shall be interpreted in accordance with their generally known meanings. Unless the context otherwise requires, words importing the singular include the plural and vice-versa; references to and use of the word “include” and its variations thereof shall mean “include without limitation” and “including without limitation”.
- 1.3. Agreement Scope and Applicability. IT IS EXPRESSLY UNDERSTOOD AND AGREED BY THE PARTIES THAT THIS AGREEMENT HAS BEEN NEGOTIATED FOR THE SPECIFIC PURPOSE OF GOVERNING SUBSCRIPTION AND PURCHASE OF THE SERVICES. PROVIDER MAY OFFER OTHER SERVICES WITH MUTUAL WRITTEN AGREEMENT BY THE PARTIES



HERETO, SUCH SERVICES MEMORIALIZED BY WAY OF AN ADDENDUM TO THIS SERVICES AGREEMENT.

All Parent branded hotels and hotels managed by Parent's Affiliates in any geographic area may purchase Services from the Company pursuant to a Work Order.

## 2. **Services**

- 2.1. This Services Agreement sets forth the terms and conditions under which Parent engages the Company for SaaS Subscription Services and or Professional Services (together the "Services") and under which it authorizes the Company to sell Services to Customers and the Company agrees to (i) grant the Parent and or Customer to access and use certain hosted services and purchase professional services offered by the Company. The Services may be provided on a single property or a portfolio basis, and may include any one or more of the following:
  - (a) A Subscription to access and use certain hosted services, or perform services, functions and responsibilities related to the hosting of the software, system and Shared Services,
  - (b) Activation, implementation, configuration and enablement of Services,
  - (c) Professional Services and other Add-Ons.
- 2.2. SaaS Subscription Services. The specific SaaS Subscription Services to be provided by the Company to the Parent or Customer will be detailed in a Work Order which will be effective when signed by the authorized parties and will be governed by the terms and conditions of this Services Agreement. In the event of any conflict between the terms and conditions set forth in this Services Agreement and the terms and conditions set out in the Work Order, the terms and conditions set out in the Work Order shall take precedence.
- 2.3. Professional Services. The specific Professional Services to be provided by the Company to the Parent or Customer will be detailed in a Scope of Work which will be effective when signed by the authorized parties and will be governed by the terms and conditions of this Services Agreement. In the event of any conflict between the terms and conditions set forth in this Services Agreement and the terms and conditions set out in the Work Order, the terms and conditions set out in the Work Order shall take precedence.
- 2.4. Customer Participation. The Services may be procured by the Parent or any Customer pursuant to the terms herein. In the event a Customer elects to engage the Services, such Customer shall execute a Work Order or a Scope of Work in the form attached hereto as Exhibit A ("**Work Order**") or in the form attached hereto as Exhibit B ("**Scope of Work**") on its own behalf, and shall be considered a separate agreement between Company and the Parent or Customer as of the date signed by authorized representatives of the Parent or Customer. Parent and the Customers agree that:
  - 2.4.1. The determination to participate hereunder by each of Parent or Customer will be completely voluntary and made in the sole discretion of the Customer, and its respective properties.





- 2.4.2. The applicable fees for the Services to be charged by the Company, including any activation fees, monthly subscription fees or Add-Ons shall be set forth in the Work Order or Scope of Work.
- 2.4.3. Upon execution of the Work Order or Scope of Work, the Customer which signs the Work Order or Scope of Work, shall be responsible for its use of the Services and for its compliance with its obligations thereunder.
- 2.4.4. It is the Parties' intent that a Work Order or Scope of Work shall not be subject to further negotiation of pricing or terms; provided, however, that the parties agree to cooperate reasonably with one another to adjust the Work Order or Scope of Work to the extent necessary to comply with the requirements of applicable laws in a particular location.
- 2.4.5. Company shall invoice the Subscriber directly for the Services provided pursuant to the applicable Work Order or Scope of Work. Charges shall be invoiced to the Subscriber pursuant to the terms of the Work Order or Scope of Work.
- 2.4.6. Parent or any Customer procuring services from Company on a trial basis shall have the option to (1) complete the trial and cease using the Services without further obligation or (2) continue the Services by entering into a Work Order or Scope of Work with Company.

### 3. **Trial or Promotion Period**

- 3.1. If the Company provides a trial, evaluation or promotion period (the "**Trial**"), the specified Services will be made available at reduced pricing until the earlier of (a) the end of the Trial for which the Customer is registered to use the applicable Services or (b) the start date of the paid Services or Subscriptions purchased by the Customer or (c) termination by the Company in its sole discretion. The Company may impose additional terms and conditions with respect to the Trial which may appear on the trial registration web page or the Work Order or Scope of Work. Any such terms and conditions are deemed incorporated into this Services Agreement by reference and are legally binding.
- 3.2. Any data entered into the Services and any customization made to the Services by the Company during the Trial will be permanently lost unless the Parties signed a Work Order or Scope of Work for the Services in consideration of payment to the Company or the Customer purchases a Subscription to the same Services.
- 3.3. During the Trial, the Services are provided on an "as-is" basis without any warranty.

### 3.4. **Confidentiality**

- 3.5. Definition of Confidential Information. As used herein, "**Confidential Information**" means all confidential and proprietary information of a party, or any of its Affiliates ("**Disclosing Party**"), disclosed to the other party, or any of its Affiliates, ("**Receiving Party**") that is marked or designated as "Confidential" and/or "Proprietary", or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure, including, without limitation, a party's business and marketing plans, technology and technical information, and business processes. Any data or information submitted by or on behalf of Customer ("**Customer Data**") is the Confidential Information of the Customer. Confidential Information (except for Customer Data)



shall not include any information that: (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party or any third party; (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party; (iii) was independently developed by the Receiving Party; or (iv) is received from a third party without breach of any confidentiality obligations.

- 3.6. **Confidentiality.** The Receiving Party shall use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (but in no event less than reasonable care) (i) to not use any Confidential Information of the Disclosing Party for any purpose outside the scope of this Agreement, and (ii) except as otherwise authorized by the Disclosing Party in writing, to limit access to Confidential Information of the Disclosing Party to those of its and its Affiliates' employees, contractors and agents ("Representatives") who need such access for purposes consistent with this Agreement and who are subject to written appropriate confidentiality obligations with the Receiving Party containing protections no less stringent than those contained herein. Receiving Party shall be liable for any breach of this Section by its Representatives.

#### 4. **Data Protection**

- 4.1. FPG will process Personal Data, as defined in the Data Processing Addendum (the "DPA") agreed upon between the Parties and attached hereto as Exhibit C, only in accordance with the provisions set forth in such DPA.

#### 5. **Term, Termination and Suspension**

- 5.1. Term of this Services Agreement. This Services Agreement shall commence on the Effective Date and, unless terminated in accordance with the termination provisions provided herein, and shall continue until the later of (i) October 19, 2025, or (ii) the stated expiration date under any extant Work Orders entered into between Customer and the Company.
- 5.2. Termination by Either Party for Cause. Subject to the terms of Section 5.5 of the GTC or any applicable termination provisions of any Work Order entered into pursuant hereto, either Party may terminate this Services Agreement on thirty (30) days' prior written notice if the other Party: (a) has committed a material breach of this Services Agreement and has failed to cure such material breach within such thirty (30) day notice period; or (b) should become insolvent, file a voluntary petition in bankruptcy, be adjudicated a bankrupt, have a receiver appointed for the operation of its business, or make a material liquidation of assets.
- 5.3. Term of the Services. The term of each of the Services or Subscription shall be as specified in the applicable Work Order or Scope of Work. Except as otherwise specified in a Work Order, Subscriptions will automatically renew for additional periods equal to the expiring Subscription term or one year (whichever is shorter), unless either party gives the other notice of non-renewal at least 30 days before the end of the term for the relevant Subscription. The per-unit pricing during any automatic renewal term will be the same as that during the immediately prior term unless the Company gives the Customer written notice of a pricing increase at least 60 days before the end of that prior term, in which case the pricing increase will be effective upon renewal and thereafter.

#### 6. **Software License Rights**

Subject to the terms of the GTC and for each valid Work Order being in full force and effect, the Company grants the contracting Parent or Customer a non-exclusive, non-transferable, non-





assignable license to access and use the FPG Software. The Company reserves all rights to the FPG Software including the right to update, modify, alter, amend or remove any functions or feature from the FPG Software at any time at its sole discretion.

**7. Publicity**

- 7.1. Customer agrees that FPG may identify Parent or Customer as a customer and use Parent's logo and trademark in FPG's promotional materials. Notwithstanding anything herein to the contrary, Parent and Customers acknowledge that FPG may disclose the existence and terms and conditions of this Services Agreement to its advisors, actual and potential sources of financing and to third parties for purposes of due diligence.
- 7.2. Order of Precedence: In the event of any conflict or inconsistency among the following, the order of precedence shall be: (1) the applicable Order Form, (2) the DPA, (3) this Services Agreement, (4) GTC.

**8. Additional Provisions**

- 8.1. After the thirty (30) day period provided in Section 5.7 of the GTC, Provider will have no obligation to maintain or provide any Customer Data and may thereafter, unless legally prohibited, delete all Customer Data. If Customer requests Provider assistance, Customer may acquire Professional Services at Provider billing rates pursuant to a separately executed Agreement.



IN WITNESS WHEREOF the Parties have entered into this Services Agreement as of the date written above.

**HARD ROCK CAFE INTERNATIONAL  
(USA), INC.**

Signature Jon Lucas

Name: Jon Lucas

Title: Chief Operating Officer

Date: November 10, 2022

**FRONTLINE PERFORMANCE  
GROUP, LLC**

Signature DocuSigned by:  
David A. Gust  
B75BD562E2C8486...

Name: David A. Gust

Title: Managing Director and CFO

Date: 10/19/2022 | 12:32 PM PDT



EXHIBIT A

“WORK ORDER - SAMPLE”



WORK ORDER - SAMPLE

Customer Address and Billing Details

Customer Name:	<input type="text"/>	Billing Entity:	<input type="text"/>
Program Sponsor:	<input type="text"/>	Billing Address:	<input type="text"/>
			<input type="text"/>
			<input type="text"/>
Sponsor Title:	<input type="text"/>	Billing Contact:	<input type="text"/>
Sponsor Email:	<input type="text"/>	Billing Contact	<input type="text"/>
		Title:	<input type="text"/>
Sponsor Phone:	<input type="text"/>	Billing Email:	<input type="text"/>
Commencement	<input type="text"/>	Billing CC Email:	<input type="text"/>
Date:	<input type="text"/>		
Recommencement	<input type="text"/>	Billing Currency:	<input type="text"/>
Date:	<input type="text"/>		

Package Services and Fees

Item	Payment Term *	Unit Price
Setup Fee	Prepayment	x,xxx.xx
Software Subscription	Monthly in advance	x,xxx.xx



## Terms and Conditions of Work Order

This Work Order is subject to Company's General Terms and Conditions (GTC) [link and Master SaaS and Services Agreement \(MSSA\) link](#). This Work Order, the MSSA and the GTC constitute the entire agreement between Company and Customer governing the Services referenced above ("Agreement"), to the exclusion of all other terms. Customer represents that its signatory below has the authority to bind Customer to the terms of this Work Order and the Agreement. The terms of this Work Order is deemed to be Confidential Information.

The Term of this Work Order is one (1) years from the Commencement Date.

THE PARTIES HERETO ACKNOWLEDGE AND AGREE THAT THE ACTUAL DAMAGES TO COMPANY IN THE EVENT OF CUSTOMER'S TERMINATION (ACTUAL OR CONSTRUCTIVE) OF THIS WORK ORDER WOULD BE IMPOSSIBLE OR IMPRACTICAL TO DETERMINE AND THAT THIS PROVISION FOR A TERMINATION FEE IS REASONABLE UNDER THE CIRCUMSTANCES EXISTING AND KNOWN TO THE PARTIES AS OF THE DATE OF THIS WORK ORDER.

The Software Subscription will auto-renew upon expiration date of the Term of this Work Order for the same Term as original provided herein (i.e., a Renewal Term of one (1) years), unless either party gives the other written notice of non-renewal at least thirty (30) days before the end of the relevant Term. A minimum of 45 days prior to the Work Order Term end, the nominated hotel representative will be emailed notification of the current active Work Order Term ending and auto renewal Term,

For services and commitments associated to professional services documented in Package Services & Fees please refer to the Packages, Deliverables & Commitments at the following [link](#)

Recommended 'best practices' to optimize your purchase can be found at the following [link](#)

Invoiced amounts for fees or services are net of any taxes. Any applicable sales or VAT taxes will be calculated and added to invoices. Any excise, withholding or other taxes are the responsibility of the Customer.

This Work Order will automatically expire thirty (30) days after the Submission Date noted above if not executed by the Customer. A revised Work Order may be issued.

Upon signature by Customer and submission to Company, this Work Order shall become legally binding unless this Work Order is rejected by Company for any of the following reasons: (1) the signatory below does not have the authority to bind Customer to this Work Order, (2) changes have been made to this Work Order (other than completion of the purchase order information and the signature block), or (3) the requested purchase order information or signature is incomplete or does not match our records or the rest of this Work Order.

If an FPG Consultant is required to travel to visit the Hotel to deliver onsite services, the Logistics Fees apply. For further details, please refer to the Logistics Fees Schedule at the following [link](#)

## Special Terms and Conditions of Work Order





## Payment Info

We wish to change the Payment Terms for Software Subscription. If no choice is selected, Payment Terms will be as indicated in Package Services & Fees above.

☐ Quarterly in advance \* ☐ Prepaid

*\* If a Customer selects 'Quarterly in advance', Customer will be billed each quarter starting on the Commencement Date, a quarterly invoice will be issued each quarter, up to the End of the Term.*

Please select Payment Method. If no choice is selected, Payment Method will default to Wire Transfer.

☐ Wire Transfer ☐ Direct Debit ☐ Credit Card \*\*

*\*\* Only for applicable countries. Corresponding Credit Card administrative fee will be included in your invoice.*

## Authorized Signatory

The Customer agrees to the terms and conditions as stated herein.

Customer Name: \_\_\_\_\_ Billing Entity: \_\_\_\_\_

\_\_\_\_\_  
Signature and Company Stamp (if applicable)

\_\_\_\_\_  
Name

\_\_\_\_\_  
Job Title

\_\_\_\_\_  
Date



**EXHIBIT B**

Scope of Work



**SCOPE OF WORK - SAMPLE**

Customer Address and Billing Details

Customer Name:	_____	Billing Entity:	_____
Program Sponsor:	_____	Billing Address:	_____
			_____
			_____
Sponsor Title:	_____	Billing Contact:	_____
Sponsor Email:	_____	Billing Contact	_____
		Title:	_____
Sponsor Phone:	_____	Billing Email:	_____
Commencement	_____	Billing CC Email:	_____
Date:	_____		
Recommencement	_____	Billing Currency:	_____
Date:	_____		

Package Services and Fees

Item	Payment Term *	Unit Price
Launch	Prepayment	x,xxx.xx
Commission @ x%	Monthly in arrears	x,xxx.xx



## Terms and Conditions of Work Order

This Scope of Work is subject to Company's General Terms and Conditions (GTC) [link and Master SaaS and Services Agreement \(MSSA\) link](#). This Scope of Work, the MSSA and the GTC constitute the entire agreement between Company and Customer governing the Services referenced above ("Agreement"), to the exclusion of all other terms. Customer represents that its signatory below has the authority to bind Customer to the terms of this Scope of Work and the Agreement. The terms of this Scope of Work is deemed to be Confidential Information.

The Term of this Scope of Work is twelve (12) months from the Commencement Date.

THE PARTIES HERETO ACKNOWLEDGE AND AGREE THAT THE ACTUAL DAMAGES TO COMPANY IN THE EVENT OF CUSTOMER'S TERMINATION (ACTUAL OR CONSTRUCTIVE) OF THIS SCOPE OF WORK WOULD BE IMPOSSIBLE OR IMPRACTICAL TO DETERMINE AND THAT THIS PROVISION FOR A TERMINATION FEE IS REASONABLE UNDER THE CIRCUMSTANCES EXISTING AND KNOWN TO THE PARTIES AS OF THE DATE OF THIS SCOPE OF WORK.

Commission, where applicable, will auto-renew upon expiration date of the Term of this Scope of Work for the same Term as original provided herein (i.e., a Renewal Term of one (1) years), unless either party gives the other written notice of non-renewal at least thirty (30) days before the end of the relevant Term. A minimum of 45 days prior to the Scope of Work Term end, the nominated hotel representative will be emailed notification of the current active Work Order Term ending and auto renewal Term,

For services and commitments associated to professional services documented in Package Services & Fees please refer to the Packages, Deliverables & Commitments at the following [link](#)

Recommended 'best practices' to optimize your purchase can be found at the following [link](#)

Invoiced amounts for fees or services are net of any taxes. Any applicable sales or VAT taxes will be calculated and added to invoices. Any excise, withholding or other taxes are the responsibility of the Customer.

This Scope of Work will automatically expire thirty (30) days after the Submission Date noted above if not executed by the Customer. A revised Scope of Work may be issued.

Upon signature by Customer and submission to Company, this Scope of Work shall become legally binding unless this Scope of Work is rejected by Company for any of the following reasons: (1) the signatory below does not have the authority to bind Customer to this Scope of Work, (2) changes have been made to this Scope of Work (other than completion of the purchase order information and the signature block), or (3) the requested purchase order information or signature is incomplete or does not match our records or the rest of this Scope of Work.

If an FPG Consultant is required to travel to visit the Hotel to deliver onsite services, the Logistics Fees apply. For further details, please refer to the Logistics Fees Schedule at the following [link](#)

## Special Terms and Conditions of Work Order





### Payment Info

Please select Payment Method. If no choice is selected, Payment Method will default to Wire Transfer.

☐

Wire Transfer

☐

Direct Debit

☐

Credit Card \*\*

*\*\* Only for applicable countries. Corresponding Credit Card administrative fee will be included in your invoice.*

### Authorized Signatory

The Customer agrees to the terms and conditions as stated herein.

Customer Name:

\_\_\_\_\_

Billing Entity:

\_\_\_\_\_

\_\_\_\_\_  
Signature and Company Stamp (if applicable)

\_\_\_\_\_  
Name

\_\_\_\_\_  
Job Title

\_\_\_\_\_  
Date



## EXHIBIT C

### Data Processing Addendum to Agreement

This Data Processing Addendum is intended to establish the terms and conditions of any Data Processing that might be performed on behalf of Controller under the Agreement. Subject to the terms and conditions of the Agreement, the Controller will determine the scope, purposes, and manner by which the Personal Data, as defined hereinafter, may be Processed and/or accessed by the Processor. The Processor will Process and/or access the Personal Data only in accordance with Controller's documented instructions as incorporated in the Agreement, this DPA, and any written instructions otherwise provided by Controller. No Personal Data will be Processed and/or accessed unless explicitly instructed in writing by the Controller.

The following exhibits are deemed part of this DPA as applicable:

- **Exhibit A** "List of Sub-Processors";

This DPA is entered to ensure that Processor's Processing of Personal Data is performed in strict compliance with all privacy and security requirements established by applicable Data Protection Laws and meets or surpasses the level of protection required by, and of the Controller.

#### TERMS AND DEFINITIONS

The following capitalized terms shall have the meaning set forth below. Terms not defined herein shall have the meaning set forth in the Agreement.

1. **"Agreement"**: means the Master Services Agreement to which this addendum is attached.
2. **"Controller"**: means the entity and/or individual who has collected the Personal Data or made the Personal Data available to Processor, and is always the one who determines the purposes and means of the Processing of Personal Data. A Controller is also known as **"Data Owner"**.
3. **"Data Protection Laws"**: means (i) all operative and applicable Laws, regulations and non-governmental standards protecting Personal Data (including but not limited to: Payment Card Industry Data Standard (PCI-DSS); Payment Application Data Security Standard (PA-DSS); the Health Insurance Portability and Accountability Act of 1996 (HIPAA)); (ii) all applicable Laws concerning collection, protection, transport, storage, use and Processing of Personal Data (including but not limited to: the California Consumer Privacy Act effective January 1, 2020 (CCPA) and its implementing regulations, as amended from time to time; the California Privacy Rights Act of 2020 (CPRA) and its implementing regulations, as amended from time to time; the Virginia Consumer Data Protection Act (VCDPA) and its implementing regulations, as amended from time to time; the Colorado Privacy Act (CPA) and its implementing regulations, as amended from time to time; the EU General Data Protection Regulation (GDPR); and the UK General Data Protection Regulation (UK GDPR)); (iii) any other applicable data security and/or data privacy Laws that apply to the Processing of Personal Data by Processor under the Agreement; and (iv) any applicable decision of the Court of Justice



of the European Union (CJEU) and any other competent judiciary authority within the field of data privacy and data security .

4. **“Data Subject”**: means an identified or identifiable natural person.
5. **“Data Subject Request”**: means a request to access, correct, amend, transfer, rectify, restrict, limit use, opt out of sale or sharing, or delete a Data Subject’s Personal Data made in accordance with applicable Data Protection Laws by the Data Subject directly or on behalf of the Data Subject by an authorized agent.
6. **“EU”**: means the European Union.
7. **“EU Adequacy Decision”**: means any decision adopted by the EU Commission determining that a third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection of Personal Data and no further specific authorization is required.
8. **“General Data Protection Regulation” or “GDPR”**: means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
9. **“Government Authority”**: means any federal, state, municipal, local, territorial, or other governmental department, regulatory authority, judicial or administrative body, whether domestic, foreign, or international.
10. **“ICO”**: means the Information Commissioner’s Office in the UK
11. **“Law”**: means any declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule recommendation or other binding restriction of or by any competent Government Authority, including Data Protection Laws.
12. **“Personal Data”**: means any information (whether in paper or electronic format) accessed or Processed under this DPA that directly or indirectly identifies or relates to a Data Subject as defined above.
13. **“Personal Data Incident” or “Incident”**: means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed, including but not limited to, security incidents that, even potentially, may lead to the following:
  - A. Unauthorized acquisition of or access to Personal Data that compromises the security, confidentiality, or integrity of the Personal Data Processed and/or stored by the Processor and/ or any of its Sub-Processors;
  - B. Disclosure of Personal Data not in the normal course of business, whether by accident or done maliciously; or
  - C. Any Incident that might compromise the security of the computing or information system(s) and/or network(s) of Controller, Processor, or Sub-Processor(s), including but not limited to: ransomware, phishing, password guessing, recording key strokes, denial-of-service, malware or virus.





14. **“Processing”**: means the Processing of Personal Data referred to as any operation or set of operations which is performed upon Personal Data, or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure or destruction.
15. **“Processor”**: means an entity or individual who is authorized by Controller to Process Personal Data on Controller’s behalf.
16. **“Service/s”**: shall have the same meaning as provided under the Agreement.
17. **“Sub-Processor”**: means a sub-contractor engaged by Processor or its affiliates to Process Personal Data in connection with the performance of the Services.
18. **“UK”**: means the United Kingdom.
19. **“UK Adequacy Decision”**: means any decision adopted by the ICO determining that a third country, where Personal Data is transferred to from UK, ensures an adequate level of protection under the UK GDPR and does not require further authorization.
20. **“UK GDPR”**: means the UK General Data Protection Regulation tailored by the Data Protection Act 2018.

### Section 1 –Personal Data

Processor will receive Personal Data from Controller or will collect Personal Data on behalf of Controller.

“Table 1- Details of Processing” below describes the details of the Processing including: (a) the categories of Personal Data that will be Processed and/or collected under this DPA; (b) the categories of Data Subjects whose Personal Data will be Processed and/or collected under this DPA; and (c ) a description of the nature, scope and purpose of the Processing.

*(Check all that apply in sections (a) and (b). Complete section (c) Scope, nature and purposes of Data Processing).*

**Table 1 – Details of the Processing (categories of Personal Data, Data Subjects and nature of the Processing)**

<p><b>a) Categories of Personal Data</b></p> <p><input type="checkbox"/> Contact Information:</p> <p>    <input checked="" type="checkbox"/> Name</p> <p>    <input type="checkbox"/> Address</p> <p>    <input type="checkbox"/> Zip Code</p> <p>    <input type="checkbox"/> Phone number</p> <p>    <input checked="" type="checkbox"/> Cell phone number</p> <p>    <input type="checkbox"/> Email address</p> <p><input type="checkbox"/> Personal Numbers:</p> <p>    <input type="checkbox"/> Date of birth</p>	<p><input checked="" type="checkbox"/> Business data (company, title, contact info)</p> <p><input type="checkbox"/> Preference information, survey answers and opinions</p> <p><input type="checkbox"/> Family and/or dependent data</p> <p>    <input type="checkbox"/> Related to customer programs</p> <p>    <input type="checkbox"/> Related to employee benefits</p> <p><input type="checkbox"/> Marital status</p> <p><input type="checkbox"/> Employment history, resume, application, references or similar</p> <p><input type="checkbox"/> Education history or records</p>
--	---



<input type="checkbox"/> Social Security or National number <input type="checkbox"/> Driver's license number <input type="checkbox"/> Tribal or state ID number <input type="checkbox"/> Passport or Visa number <input type="checkbox"/> Other <input type="checkbox"/> Financial: <input type="checkbox"/> Records <input type="checkbox"/> Bank Account or credit card numbers <input type="checkbox"/> Pins/passwords/access code <input type="checkbox"/> Security questions/answers <input type="checkbox"/> Web / Digital / Tracking Information: <input type="checkbox"/> IP address <input type="checkbox"/> Cookies <input type="checkbox"/> Browser history or page views <input type="checkbox"/> Mobile device ID or type <input type="checkbox"/> Geolocation <input type="checkbox"/> Social network, 'handle' data <input type="checkbox"/> Biometric Information: <input type="checkbox"/> Fingerprint recognition <input type="checkbox"/> Iris recognition <input type="checkbox"/> Facial recognition <input type="checkbox"/> Voice and speech recognition <input type="checkbox"/> Signature recognition	<input type="checkbox"/> Insurance information <input type="checkbox"/> Medical, health, mental or similar data <input type="checkbox"/> Physical description, biometric, genetic or similar type data <input type="checkbox"/> Gender <input type="checkbox"/> Beneficiary information <input type="checkbox"/> Religion <input type="checkbox"/> Origin/Race/Ethnicity <input type="checkbox"/> Union membership, status, or related data <input type="checkbox"/> Sexual life, orientation <input type="checkbox"/> Criminal offences, allegations, proceedings, or other related information <input type="checkbox"/> Audio, electronic, visual, thermal, olfactory, or similar information <input type="checkbox"/> Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.  <u>Controller's Confidential Business Information</u> <input type="checkbox"/> Financial records <input type="checkbox"/> Identification of customers <input type="checkbox"/> Information relating to Controller's processes or operations <input type="checkbox"/> Employee records <input type="checkbox"/> Other:  Other Data: X. Personal Data transfer only relates to associates of the the hotel. No hotel guest personal data is transferred. Work Mobile Number are personal choices of entry.
--	--

<b>b) Categories of Data Subjects</b> <input type="checkbox"/> None <input checked="" type="checkbox"/> Employee information <input type="checkbox"/> Customer information	Add details here:
---	-------------------





<input type="checkbox"/> Processor information <input type="checkbox"/> End user information <input type="checkbox"/> Job Applicant information <input type="checkbox"/> Police/Fire information <input type="checkbox"/> Other categories of Data Subjects	Personal data is limited to the application end users who are predominantly front desk agents involved in the checkin process
---	---

**c) Scope, nature and purposes of Data Processing:**

The processing will be to facilitate the performance of the services as set forth in the written services agreement with the (sub-) processor, for the duration of the performance of the services as set forth in the written services agreement with the (sub-) processor.

**Section 2 – Processor Processing of Personal Data**

Processor agrees to the following:

1. To collect and/or store only the Personal Data that Controller has consented to share with Processor.
2. The Personal Data may only be Processed for the limited and specific purpose as identified in Controller's documented instructions, the Agreement, this DPA, or consent, as applicable, provided by Data Subjects. Should the Processor reasonably believe that a specific Processing activity beyond the scope of Controller's instructions is required to comply with a legal obligation to which Processor is subject, the Processor shall inform Controller of that legal obligation and seek explicit authorization from Controller before undertaking such Processing. Processor shall never Process the Personal Data in a manner inconsistent with Controller's documented instructions.
3. Processor is a service provider using Personal Data for a business purpose as defined under the California Consumer Privacy Act ("CCPA") to the extent that CCPA applies to this DPA. Processor shall not sell (as such term is defined in the applicable Data Protection Law) and/or share the Personal Data and/or retain, use, or disclose the Personal Data for any other customer or client, or for any commercial purposes other than providing the Services to Controller under the Agreement and this DPA. Notwithstanding anything to the contrary in this DPA or the Agreement, Controller and Processor acknowledge and agree that Processor's access to the Personal Data is not part of the consideration exchanged by the Parties in respect of this DPA or the Agreement.
4. When Processing Personal Data, that by its nature, is sensitive or poses high risk, Processor shall identify the Personal Data involved, assign appropriate levels of authorization to access such Personal Data based on what is strictly necessary, adopt heightened security measures at





all phases of the Processing including, but not limited to data transfer, maintenance, retention, and/or destruction of the Personal Data.

5. If Processing relies on the consent of the Data Subject, and such consent is withdrawn, Processor shall immediately stop all Processing related to that Data Subject upon notice by Controller and take immediate action to have its Sub-Processors immediately stop all Processing of such Data Subject's Personal Data.
6. Processor shall ensure that all of its employees, agents and/or Sub-Processors engaged in the Processing of Personal Data under this DPA are informed of the confidential nature of the Personal Data. Processor shall also ensure that all such persons have received the appropriate training regarding their responsibilities, and have executed a written confidentiality agreement or are under an appropriate statutory obligations of confidentiality. Processor shall take commercially reasonable steps to ensure the reliability of all such persons engaged in the Processing of Personal Data. Processor shall ensure that access to Personal Data is granted to members of its personnel only to the extent strictly necessary for implementing, managing, and monitoring the Services under the Agreement.
7. Except as provided in Section 3, Processor shall not share any Personal Data with any third-party, including but not limited to Processor's Sub-Processors or any other processors engaged by Controller without obtaining prior written consent of Controller.
8. Processor shall not Process or transfer any Personal Data in or to a territory other than the territory in which it received the Personal Data from Controller or, to the extent applicable, the territory where it collected the Personal Data, unless it takes measures to ensure that such Processing or transfer is in compliance with the applicable Data Protection Laws and with the prior written authorization of Controller.
9. Processor shall not combine Personal Data received from Controller with any other information Processor receives from or on behalf of another person or business or which it collects from its own interactions with Data Subjects.
10. If at any time Processor determines that it is unable to comply with or maintain the terms of this DPA or the Agreement, Processor shall notify Controller within seventy-two (72) business hours. In the event Processor is in breach of its obligations under this DPA, Controller's instructions provided in writing, and/or applicable Data Protection Laws, Controller may instruct the Processor to suspend the Processing of Personal Data until the Processor achieves compliance or the Agreement is terminated. Further, Controller may take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data.
11. Upon Controller's request, Processor shall provide Controller with all reasonable cooperation and assistance needed by Controller in complying with the following obligations, taking into account the nature of the Data Processing and the information available to the Processor: (i) completing any data privacy risk assessment required by Controller for the purpose of internal due diligence; (ii) completing the data protection impact assessments ("DPIA") that may be required under applicable Data Protection Laws; (iii) completing the transfer impact assessment ("TIA") when the Processing under this DPA may include a cross-border data



transfer: (iv) consulting with any competent supervisory authorities under applicable Data Protection Laws; and (v) ensuring that Controller's Personal Data is accurate and up to date.

### **Section 3 – Sub-Processors**

1. Processor shall not engage any other processor to perform any of its Services-related activities under the Agreement, consisting in whole or in part of the Processing of the Personal Data or requiring Personal Data to be Processed by any Sub-Processor without the prior written authorization of Controller.
2. Controller authorizes Processor to engage the Sub-Processors listed in Exhibit A for the Service-related Personal Data Processing activities described in the Agreement or this DPA, limited to the scope described in such Exhibit A with reference to each Sub-Processor. Prior to engaging a new Sub-Processor or replacing an existing one, Processor shall inform the Controller of such change in writing and give Controller a reasonable opportunity to object to such change. If Controller timely sends Processor a written objection notice, setting forth a reasonable basis for objection, the Parties will make a good-faith effort to resolve Controller's objection. In the absence of a resolution, Processor shall make reasonable efforts to provide Controller with the same level of service described in the Agreement, without using the suggested Sub-Processor to Process Controller's Personal Data. If Processor's efforts are not successful within a reasonable time, each Party may terminate the portion of the Services which cannot be provided without the Sub-Processor, and Controller will be entitled to a pro-rated refund of the applicable service fees from the date of its objection.
3. Processor shall ensure that any Sub-Processor that has access to Personal Data under this DPA executes a written agreement obligating the Sub-Processor to comply with terms and conditions at least as restrictive as those imposed on Processor under this DPA, the Agreement, and applicable Data Protection Laws. Furthermore, Processor shall supervise compliance with such agreement and ensure that any Sub-Processor implements appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of applicable Data Protection Laws. Processor shall notify the Controller of any failure by the Sub-Processor to fulfill its contractual obligations.
4. Notwithstanding any authorization by Controller within the meaning of the preceding paragraph, to the extent any Sub-Processor fails to fulfill its obligations, Processor shall remain fully liable to Controller for the performance of any such Sub-Processor's obligations.
5. Controller may request that Processor audit a Sub-Processor or provide confirmation that such an audit has occurred, or, where available, obtain or assist Controller in obtaining a Processor audit report concerning the Sub-Processor's operations to ensure compliance with its obligations imposed by Processor in conformity with this DPA and the Agreement.

### **Section 4 – Transfer of Personal Data to Third Countries**





1. Processor shall promptly notify Controller of any planned, permanent or temporary transfers of Personal Data to a third country outside of the ordinary course of business, and shall only perform such a transfer after obtaining written authorization from Controller, which may be refused at Controller's discretion, and pursuant to documented instructions from Controller.
2. If any of the data transfer mechanisms described above is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, Controller and Processor agree to cooperate in good faith to promptly suspend the transfer of Personal Data or to pursue a suitable alternate mechanism, such as binding corporate rules if applicable, that is a recognized compliance standard and that can lawfully support the transfer. If the Parties cannot find a suitable alternate mechanism, either party may terminate the Agreement by providing written notice to the other party, and the Controller will be entitled to a pro-rated refund of the applicable service fees.

#### **Section 5 –Data Retention/Data Destruction**

1. Processor shall take appropriate measures to comply with the data retention and data destruction requirements in this DPA or applicable Data Protection Laws, whichever is stricter. Processor shall retain the Personal Data no longer than is necessary to Process such Personal Data or complete the Services agreed to in the Agreement unless otherwise specified. If the Personal Data must be stored or retained by Processor, Processor shall de-identify, encrypt, or implement any other comparable measures to protect the Personal Data.
2. If Processor disposes of any paper or electronic record containing Personal Data, Processor will do so in an appropriate manner under this DPA or as specified by applicable Data Protection Laws, whichever is stricter, to prevent unauthorized access in connection with its disposal.
3. At any time during the term of the Agreement, Controller may make a written request to Processor to permanently delete, retrieve, and/or destroy some or all of the Personal Data related to Processor's Services under the Agreement and Processor shall certify compliance with such request upon completion, and will describe any exceptions.
4. The Parties agree that on the termination of the Agreement, Processor shall at the choice of Controller and under Controller's written instructions: (i) return all Personal Data Processed including any copies thereof to Controller and, after returning such Personal Data and without undue delay, securely destroy any copy of Personal Data that might be still stored in the system of the Processor or its Sub-Processors; or (ii) securely destroy all the Personal Data without undue delay. In both situations (i) and (ii) above, immediately after destruction of the Personal Data, Processor shall certify in writing to Controller that all forms of Personal Data and related copies if any have been permanently destroyed in accordance with the standards set forth in this DPA and any other additional instructions provided by Controller and will describe any exceptions thereto.
5. If Processor is prevented by applicable Laws from returning or destroying all or part of the Personal Data Processed, Processor shall provide written notification to the Controller





describing all exceptions and obligations under such applicable Laws and providing warranties that Processor will properly safeguard the confidentiality of the Personal Data in accordance with applicable Data Protection Laws and this DPA stopping and not resuming any Processing of the Personal Data. If Processor returns the Personal Data to Controller, Processor is still required to destroy any back-ups of Personal Data that it may have retained. The Parties agree that Section 8 , (“Security”) of this DPA shall continue to apply to the retained Personal Data for as long as it is retained by Processor under this Section. Personal Data shall be returned to Controller in its native format or within a common computer delineated file.

6. If Controller becomes subject to a duty to preserve (or halt the destruction of) documents once litigation, an audit or a government investigation is reasonably anticipated, Processor shall be notified. Processor shall immediately cease all document destruction for the Personal Data specified by Controller.
7. Processor shall notify all Sub-Processors supporting its own Processing of the Personal Data of the termination of the DPA and will warrant that all such Sub-Processors will either destroy the Personal Data or return the Personal Data to Controller, in accordance with the instructions provided by Controller.

#### **Section 6 – Right To Audit**

1. At Controller’s request, Processor shall demonstrate compliance with this DPA, as well as any applicable Data Protection Laws and industry standards by providing adequate documentation as determined by Controller in its sole discretion. Controller, or an appointed audit firm (Auditor), also has the right to audit Processor’s compliance with its obligations under this DPA and the Processing, transport, or storage of Controller’s Personal Data.
2. Controller will announce the intent to audit Processor by providing at a minimum four weeks notice to Processor. Thereafter, Processor can elect to either provide an audit report from an audit within the 12 prior months, or elect to allow Controller to proceed with its own audit, which will progress as follows: a document specifying the scope and deliverables to be expected from the audit will be provided to Processor at the time Processor is notified of the audit. The audit is limited to those systems of Processor used for providing the Service(s) to or supporting Controller. If the documentation requested cannot be removed from Processor’s premises, Processor will allow the Auditor access to its site and allow for a reasonable workspace and Internet connectivity. Processor will make necessary employees or contractors available for interviews in person or on the phone during the time frame of the audit.
3. In lieu of Controller or Controller’s appointed audit firm performing the audit, if Processor has an external audit firm that performs a certified review that is directly applicable to this DPA, such as SOC2, Type II audit of data security controls or a SOC1, Type I audit of financial controls (or a SSAE 16 audit of financial controls) Controller may choose to review the reports incorporating the audit results. Controller reserves the right to determine if such certified reports are sufficient for the purpose of the audit.



4. Processor shall provide reasonable supporting documentation regarding its data safeguards, data access audits, user access audits, business continuity and disaster facilities, resources, plans, policies/procedures, and employee training within the limitation and in connection with the type of Services being provided to the Controller under the Agreement. It is understood that nothing in this Section 6 shall require Processor to breach any duty of confidentiality owed to any of its other customers and/or its employees.
5. Controller vulnerability and application scanning: Processor agrees to perform, through a certified security assessment company or a Processor's qualified personnel, both to be approved by Controller, a vulnerability and application scanning test at least once a year and take prompt corrective action(s) to remediate any vulnerabilities or security concerns identified by Processor or otherwise identified vulnerabilities that may affect Controller's Personal Data. Corrective action(s) must be implemented in a timeframe commensurate with industry standards or as agreed upon with Controller. Controller acknowledges that additional costs to remediate/mitigate vulnerabilities may be incurred when said vulnerabilities are not due to negligence or other circumstances where Processor is not at fault. If such costs are judged by Controller to be unacceptable, Controller may terminate the Agreement with Processor.

#### **Section 7 – Data Subjects' Rights**

1. Processor shall assist Controller in fulfilling Controller's obligations under applicable Data Protection Laws to respond to Data Subject Requests by providing the information requested by Controller or taking any reasonable action as requested by Controller.
2. Processor shall respond to Controller within seventy two (72) business hours in relation to the following request(s):
  - a) Provide a copy of all of Personal Data related to the Data Subject;
  - b) Modify, correct, or otherwise alter the Personal Data as instructed and ensure that its Sub-Processors do the same;
  - c) Remove, erase, delete, or otherwise destroy the Personal Data and ensure that its Sub-Processors do the same;
  - d) Stop all Processing – and ensure any Sub-Processor ceases all Processing - of the Data Subject's Personal Data when consent has been withdrawn;
  - e) Specific instructions issued by a lawful request by a public authority.
3. Processor shall comply with Controller's instructions to delete Personal Data Processed under the Agreement and shall notify any Sub-Processors of such direction as applicable, provided, however, Processor shall not be required to delete any of the Personal Data to comply with a Data Subject's request directed by Controller if it is necessary to maintain such information in accordance with applicable Data Protection Laws, in which case, Processor shall promptly inform Controller of the exceptions relied upon under the applicable Data Protection Law and Processor shall not use the Personal Data retained for any other purpose than provided for by such exception.





4. If Processor is unable to comply with any of the above, Processor must provide a reason within forty eight (48) business hours to Controller.
5. Processor shall notify Controller within seventy two (72) business hours if it receives any of the above-identified requests directly from a Data Subject. Processor shall not respond to the Data Subject, unless authorized in writing by the Controller to do so.

## **Section 8 – Security**

1. In addition to any security measures agreed upon and described in the Agreement, Processor shall:
  - a) Take appropriate actions to protect the Personal Data from any unauthorized use, access, disclosure, alteration, or destruction including, but not limited to, implementing network security controls that conform to generally recognized industry standards and best practices to protect and maintain the security of all Personal Data collected, handled, Processed or otherwise used or accessed by Processor. Processor shall regularly monitor these measures to ensure that they meet the requirements of applicable Data Protection Laws, and it shall ensure that the measures implemented protect Data Subjects' rights. Processor shall not materially decrease the security measures during the term of the Agreement.
  - b) No more than once a calendar year, promptly and accurately complete a written information security questionnaire provided by Controller or a third party on Controller's behalf regarding Processor's business practices and information technology environment in relation to all Personal Data being accessed, handled, Processed or stored and/or Services being provided by Processor to the Controller
  - c) Periodically be subject to audit to ensure compliance with minimum data privacy and protection standards required by applicable Data Protection Laws.
  - d) Comply with certified IT management frameworks such as ISO 27001, NIST, or any other equivalent framework in accordance with applicable industry standards and applicable Laws in order to ensure sufficient care and protection of all Personal Data Processed on behalf of Controller. In particular, Processor shall design and implement an Information Security Program, which will include administrative, technical and physical safeguards appropriate to the size and complexity of Processor's business and the nature and scope of the Services to be performed, as well as the likelihood and severity of the risk to the rights and freedoms of Data Subjects, in order to ensure the confidentiality, integrity and availability of the Personal Data, and the by-products of such information. The Information Security Program shall address, among other things, the initial risk assessment, risk management and control, risk mitigation plan, training of Processor's employees and/or agents on the Information Security Program, testing of the Information Security Program, oversight of any Processor arrangements, periodic reports to Controller upon request, and the process for annual certification of





- Processor. The Information Security Program shall also include written policies and procedures designed to detect, assess, control and respond to any unauthorized and/or unlawful access to the Personal Data. Processor shall adopt security measures, including but not limited to: access controls, encryption, audit logging and/or other means, where appropriate, taking into account the risks that are presented by Processing, including without limitation the risks of a Security Incident, the nature of the Personal Data involved, the size of the Processor, and the likelihood of Security Incidents.
- e) Maintain a business continuity plan as well as production and disaster recovery systems in geographically dispersed secured SOC2 certified datacenters in the United States with redundancy on all critical support elements (i.e. data, power, environmental controls, and fire suppression).
  - f) Agree and ensure that no Personal Data, including sensitive data, will cross publicly accessible networks in unencrypted or plain text formats.
  - g) Store all Controller backup data, including Personal Data, as part of Processor's designated automatic backup and recovery processes in encrypted form, using a commercially supported encryption solution.
  - h) Agree and ensure that any and all Personal Data stored on any portable or laptop computing device or any portable storage medium is likewise encrypted.
  - i) To any extent that in providing the Services Processor has access to Controller's computing environment (the "**Controller System**") (which includes, without limitation, Processor's transmission or storage of electronic files or other electronic data to the Controller System), Processor shall meet all commercially reasonable technological security standards, including, but not limited to, the use of computer firewalls, strong user authentication, encrypted transmissions and storage, anti-malware programs, regular and timely software security patch application, and controlled access to the physical location of computer hardware, to protect Personal Data and the Controller System against any damage, disruption or interference from any destructive computer programming including, but not limited to, harmful computer instructions, viruses, Trojan horses, and worms introduced by or through any hardware or software delivered or used by Processor.
  - j) Any and all Personal Data will be stored, Processed, and maintained solely on designated target servers and that no Personal Data at any time will be Processed on or transferred to any portable or laptop computing device or any portable storage medium, unless that storage medium is in use as part of the Processor's designated backup and recovery processes.
  - k) Ensure that no Personal Data is accessed, stored, transmitted or transported to or from any information systems outside of the United States except as necessary for the provision of services by Processor; provided that: (i) Processor shall store the Personal



Data in the appropriate location where applicable Data Protection Laws require that Personal Data be stored in a jurisdiction other than the United States; and (ii) Controller expressly requests in writing that Processor store Personal Data in a location other than United States.

- 1) In order to ensure the ability to investigate security incidents, make available detailed logging of its transactions, including but not limited to: (i) privileged access to any sensitive information, including IP addresses of the user and original user name; (ii) account creation, deletions, and modifications; (iii) failed attempts to access Personal Data; (iv) all Logins (failed and successful) with IP address, using date, time, and user ID; (v) any operating system ("OS") patch or OS configuration changes and the user and IP address making them; (vi) any changes to files in the web application directories and the user and IP address making them; (vii) any log file deleted and the user and IP address making the change; (viii) any log file changed by the non-owing process and the user and IP address making the change; (ix) Service start/stop of any service, system, or server (i.e., any reboot of service or server outside of the normal maintenance window); and (x) changes to firewall configuration files and the user and IP address making the changes.
2. It is presumed that the consequences of a virus, Trojan, or worm infection; intrusion by unauthorized third-parties; or similar security incidents are the mutual responsibility of both Processor and Controller. Both Parties agree to retain all authentication logs for a minimum of three (3) months from the creation of such logs as well as run up-to-date, commercially-available enterprise antivirus/malware detection and prevention software on their systems. Additionally, both Parties agree to cooperate with each other in case of a Personal Data Incident which will require collaboration and communication to identify potential threats that may cause harm or other negative impact to either Party.

## **Section 9 – Incident Response Plan**

1. Processor shall:
  - a) Have an Incident Response Plan to respond to all actual and potential Incidents having an impact on Personal Data and/or security. In the event of an Incident, or threat of an Incident, Processor shall take the actions set out in suchs Incident Response Plan.
  - b) Provide Controller, not later than the execution date of this DPA if not already indicated below in this section, with the name and contact information of the Processor's Data Protection Officer (DPO) or other employee of Processor who shall serve as Controller's primary security contact and who shall be available to assist Controller as a contact in resolving obligations associated with any Incident that might occur in connection with the Services;

Processor's Security Contact Information:

Name: Data Protection Office





Phone: +1 407 682 3434

Email: [DataProtection@frontlinepg.com](mailto:DataProtection@frontlinepg.com)

2. In the instance of a confirmed or suspected Incident that compromises Controller's Personal Data or puts Controller's Personal Data at risk, Processor shall report such Incident to Controller's Security contact, as indicated below, within twenty-four (24) hours of discovery of the Security Incident to allow Controller to meet reporting timeframes mandated by applicable Data Protection Laws.
3. When reporting the Incident, Processor shall NOT include in its notification any of the Personal Data that was a part of the confirmed or suspected Incident in the notification;

Controller's Security Contact Information:

GDPRO - Global Data Protection & Risk

Name: Office

Phone: +1 (954) 498-9834

Email: [dataprotection@hardrock.com](mailto:dataprotection@hardrock.com)

4. The notification under sub-section 2 above shall contain the following: (i) description of the nature of the Incident, including, where possible, the categories of Personal Data and approximate number of data records and Data Subjects involved; (ii) the contact person within Processor's organization to obtain more information if such contact is someone other than the Processor Security contact listed above; (iii) the likely impact of the Incident and the measures taken or planned to be taken to address the Incident and mitigate its effects.
5. Immediately following Processor's notification to Controller of the Incident, the Parties shall coordinate with each other to investigate the Incident. Processor agrees to fully cooperate with Controller in Controller's handling of the matter, including, without limitation:
  - i. Assisting Controller with any investigation;
  - ii. Providing Controller with physical access to the facilities and operations affected;
  - iii. Facilitating interviews with Processor's employees and others involved in the matter; and
  - iv. Making available all relevant records, logs, files, data reporting and other materials required to comply with applicable Data Protection Laws, industry standards or as otherwise reasonably required by Controller.
6. Controller will not expect Processor to divulge proprietary business information.
7. Processor shall use best efforts to immediately remedy any Incident and prevent any further Incident at Processor's expense in accordance with applicable Data Protection Laws.





Processor shall reimburse Controller for actual costs incurred by Controller in responding to, and mitigating damages caused by, any confirmed or potential Incident, including all costs of notice and/or remediation.

8. Unless otherwise agreed by the Parties in writing, Processor shall provide Controller with updated information on a regular basis until any actual or suspected Incident and investigation has been resolved.
9. Processor agrees that it shall not inform any third party of any Incident without first obtaining Controller's prior written consent, other than to inform a complainant that the matter has been forwarded to the Controller's legal counsel. Further, Processor agrees that Controller shall have the sole right to determine:
  - A. Whether notice of the Incident is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others as required by applicable Data Protection Laws, or otherwise in Controller's discretion; and
  - B. The contents of such notice, whether any type of remediation may be offered to affected Data Subjects, and the nature and extent of any such remediation.
10. Processor agrees to fully cooperate at Controller's expense with Controller in any litigation or other formal action deemed reasonably necessary by Controller to protect its rights relating to the use, disclosure, protection and maintenance of the Personal Data.
11. Processor agrees to promptly use its best efforts to prevent a recurrence of any such Incident.
12. Processor will maintain records of any confirmed or potential Incidents in accordance with commercially accepted industry practices, and will make such records available to Controller upon request.

## **Section 10 – Services Interruption**

1. In the event of any dispute, default, litigation, or claim, or for any another reason that Processor may wish to terminate the Agreement, stop providing the Services, or withhold information, (collectively to be known as a “**Service Interruption**”), Processor agrees that:
  - a) Controller shall continue to be the sole owner of the Personal Data and retain all right, title, and interest in and to the Personal Data;
  - b) Processor shall continue to provide all administrative, technical, and physical safeguards with respect to the Personal Data of Controller;
  - c) The Service Interruption will not halt or pause any Processor restrictions to the Personal Data;
  - d) Processor shall continue to assist Controller in fulfilling its obligations in connection with Data Subject Requests:



- e) All provisions set forth in Sections 8 and 9 above of this DPA shall continue to apply; and
- f) If there is no recourse to the Service Interruption, Controller maintains the right to request that Processor purge, retrieve, and/or destroy some or all of the Personal Data to ensure that all control of the Personal Data is returned to the Controller.

## **Section 11 – Regulatory Authority Requests and Enforcement**

1. Processor shall assist Controller in communicating and cooperating with any Regulatory Authority in connection with Controller's Personal Data.
2. Processor shall notify Controller of all inquiries from a Regulatory Authority that Processor receives which are related to the Processing of Personal Data under the Agreement, the provision or receipt of the Services, or either party's obligations under the Agreement, unless prohibited from doing so by law or by the Regulatory Authority.
3. Unless a Regulatory Authority requests in writing to engage directly with the Processor, the Parties (acting reasonably and taking into account the subject matter of the request), agree that Controller shall be responsible for handling all requests. Controller shall: (a) be responsible for all communications or correspondence with the Regulatory Authority in relation to the Processing of Personal Data and the provision or receipt of the Services, and (b) keep Processor informed of such communications or correspondence to the extent permitted by law. Processor shall provide such commercially reasonable assistance as Controller may request in relation to such a Regulatory Authority's request.

## **Section 12 – Liability and Indemnity**

Subject to the limitations contained in the Agreement, Processor shall indemnify Controller and holds Controller harmless against all costs, claims, actions, demands, losses, damages, fines, penalties and expenses including but not limited to attorneys' fees, incurred by Controller arising out of or in connection with Processor's or a Sub-Processor's breach of any provision of this DPA or applicable Data Protection Laws, and Controller shall indemnify Processor and holds Processor harmless against all costs, claims, actions, demands, losses, damages, fines, penalties and expenses including but not limited to attorneys' fees, incurred by Processor arising out of or in connection with Controller's breach of any provision of this DPA or applicable Data Protection Laws.

## **Section 13 – Term and Termination**



This DPA shall come into effect on the effective date of the Agreement. Processor shall Process Personal Data until the date of expiration or termination of the Agreement, whichever is earlier, unless instructed otherwise by Controller, or until such Personal Data is returned or destroyed on instruction of Controller.





## **Exhibit A**

### **List of Sub-Processors**

This Exhibit A incorporates below the list of Sub-Processors that are have been expressly authorized by Controller to Process and/or access Personal Data on behalf of Processor in accordance with the terms of the DPA and the documented instructions provided by Controller, and solely in connection with the Services performed under the Agreement entered into by and between Controller and Processor.

Any change to the following list shall be agreed upon by both Parties in writing and memorialized in a written amendment to this Exhibit A.

Sub-Processor Name	Sub-Processor State of Incorporation	Sub-Processor Physical Address	Sub-Processor DPO or Data Privacy representative Contact (including name, title, e-mail and phone number)	Description of services provided to the Processor in connection with the Agreement and the Data Processing involved
Amazon Web Services, Inc.	Delaware, USA	410 Terry Avenue North Seattle, WA 98109 United States	Jordan Petrozzino, Account Executive, +18505245374	Amazon Web Services, Inc. provides information technology services.
Accion Labs	Pennsylvania, USA	1225 Washington Pike #401, Bridgeville, PA 15017	Ramesh Narasimha, COO, +1-724-260-5139	Accion Labs provide outsourced architects and engineers which support our infrastructure: a. Primarily working on ETL Architecture b. Data Lake services



				<div>c. Managed solutions</div> <div>d. Data processing</div>
--	--	--	--	---

**Certificate Of Completion**

Envelope Id: C5CC7B2BBFDE4CFF9C57DCEDE8C1E0DC

Status: Delivered

Subject: Complete with DocuSign: Frontline\_HRI - MSA SaaS - HRI 4882-6661-8413 v.3.docx

Source Envelope:

Document Pages: 31

Signatures: 1

Envelope Originator:

Certificate Pages: 5

Initials: 0

Katz Teller

AutoNav: Enabled

255 East Fifth Street

Envelope Stamping: Enabled

Suite 2400

Time Zone: (UTC-08:00) Pacific Time (US &amp; Canada)

Cincinnati, OH 45202

DocuSignCorporate@katzteller.com

IP Address: 66.117.203.162

**Record Tracking**

Status: Original

Holder: Katz Teller

Location: DocuSign

10/19/2022 12:13:32 PM

DocuSignCorporate@katzteller.com

**Signer Events**

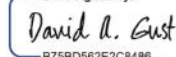
David A. Gust

dgust@frontlinepg.com

Managing Director and CFO

Security Level: Email, Account Authentication  
(None)**Signature**

DocuSigned by:



B75BD562E2C8486...

Signature Adoption: Pre-selected Style

Using IP Address: 184.88.235.246

Signed using mobile

**Timestamp**

Sent: 10/19/2022 12:16:38 PM

Viewed: 10/19/2022 12:31:59 PM

Signed: 10/19/2022 12:32:22 PM

**Electronic Record and Signature Disclosure:**

Accepted: 10/19/2022 12:31:59 PM

ID: 4c48d58b-1b18-409b-acc6-1061c7710dc5

Jon Lucas, COO

contractadministration@shrss.com

Security Level: Email, Account Authentication  
(None)

Sent: 10/19/2022 12:16:38 PM

Viewed: 10/20/2022 8:26:21 AM

**Electronic Record and Signature Disclosure:**

Accepted: 10/20/2022 8:26:21 AM

ID: ea966519-c84e-46db-bcdd-1b44ab3faf93

**In Person Signer Events****Signature****Timestamp****Editor Delivery Events****Status****Timestamp****Agent Delivery Events****Status****Timestamp****Intermediary Delivery Events****Status****Timestamp****Certified Delivery Events****Status****Timestamp****Carbon Copy Events****Status****Timestamp**

Amy Butcher

abutcher@frontlinepg.com

Security Level: Email, Account Authentication  
(None)**COPIED**

Sent: 10/19/2022 12:16:38 PM

Viewed: 10/19/2022 12:22:33 PM

**Electronic Record and Signature Disclosure:**

Not Offered via DocuSign



Carbon Copy Events	Status	Timestamp
Gabriel Kurcab gkurcab@katzteller.com Officer Security Level: Email, Account Authentication (None) <b>Electronic Record and Signature Disclosure:</b> Accepted: 10/3/2022 10:27:12 AM ID: dd34278a-3f48-4477-be2f-6b9338b9a76f	COPIED	Sent: 10/19/2022 12:16:39 PM
Miguel Aguirre miguel.aguirre@shrss.com Security Level: Email, Account Authentication (None) <b>Electronic Record and Signature Disclosure:</b> Not Offered via DocuSign	COPIED	Sent: 10/19/2022 12:16:37 PM Viewed: 11/2/2022 2:26:32 PM
Tom Coman TComan@frontlinepg.com Security Level: Email, Account Authentication (None) <b>Electronic Record and Signature Disclosure:</b> Not Offered via DocuSign	COPIED	Sent: 10/19/2022 12:16:39 PM Viewed: 10/19/2022 12:17:29 PM

Witness Events	Signature	Timestamp
Notary Events	Signature	Timestamp
Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	10/19/2022 12:16:39 PM
Certified Delivered	Security Checked	10/20/2022 8:26:21 AM
Payment Events	Status	Timestamps
Electronic Record and Signature Disclosure		

## **CONSUMER DISCLOSURE**

From time to time, Katz Teller Brant Hild (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign, Inc. (DocuSign) electronic signing system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to these terms and conditions, please confirm your agreement by clicking the "I agree"™ button at the bottom of this document.

### **Getting paper copies**

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after signing session and, if you elect to create a DocuSign signer account, you may access them for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a \$0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

### **Withdrawing your consent**

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

### **Consequences of changing your mind**

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. To indicate to us that you are changing your mind, you must withdraw your consent using the DocuSign "Withdraw Consent"™ form on the signing page of a DocuSign envelope instead of signing it. This will indicate to us that you have withdrawn your consent to receive required notices and disclosures electronically from us and you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

### **All notices and disclosures will be sent to you electronically**

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures



electronically from us.

**How to contact Katz Teller Brant Hild:**

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: [ktbh@katzteller.com](mailto:ktbh@katzteller.com)

**To advise Katz Teller Brant Hild of your new e-mail address**

To let us know of a change in your e-mail address where we should send notices and disclosures electronically to you, you must send an email message to us at [ktbh@katzteller.com](mailto:ktbh@katzteller.com) and in the body of such request you must state: your previous e-mail address, your new e-mail address. We do not require any other information from you to change your email address..

In addition, you must notify DocuSign, Inc. to arrange for your new email address to be reflected in your DocuSign account by following the process for changing e-mail in the DocuSign system.

**To request paper copies from Katz Teller Brant Hild**

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an e-mail to [ktbh@katzteller.com](mailto:ktbh@katzteller.com) and in the body of such request you must state your e-mail address, full name, US Postal address, and telephone number. We will bill you for any fees at that time, if any.

**To withdraw your consent with Katz Teller Brant Hild**

To inform us that you no longer want to receive future notices and disclosures in electronic format you may:

- i. decline to sign a document from within your DocuSign session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;
- ii. send us an e-mail to [ktbh@katzteller.com](mailto:ktbh@katzteller.com) and in the body of such request you must state your e-mail, full name, US Postal Address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

**Required hardware and software**

Operating Systems:	Windows® 2000, Windows® XP, Windows Vista®; Mac OS® X
Browsers:	Final release versions of Internet Explorer® 6.0 or above (Windows only); Mozilla Firefox 2.0 or above (Windows and Mac); Safari®, 3.0 or above (Mac only)
PDF Reader:	Acrobat® or similar software may be required to view and print PDF files
Screen Resolution:	800 x 600 minimum
Enabled Security Settings:	Allow per session cookies

\*\* These minimum requirements are subject to change. If these requirements change, you will be asked to re-accept the disclosure. Pre-release (e.g. beta) versions of operating systems and browsers are not supported.

**Acknowledging your access and consent to receive materials electronically**

To confirm to us that you can access this information electronically, which will be similar to

other electronic notices and disclosures that we will provide to you, please verify that you were able to read this electronic disclosure and that you also were able to print on paper or electronically save this page for your future reference and access or that you were able to e-mail this disclosure and consent to an address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format on the terms and conditions described above, please let us know by clicking the "I agree"™ button below.

By checking the "I agree"™ box, I confirm that:

- I can access and read this Electronic CONSENT TO ELECTRONIC RECEIPT OF ELECTRONIC CONSUMER DISCLOSURES document; and
- I can print on paper the disclosure or save or send the disclosure to a place where I can print it, for future reference and access; and
- Until or unless I notify Katz Teller Brant Hild as described above, I consent to receive from exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to me by Katz Teller Brant Hild during the course of my relationship with you.