DATA PROCESSING AGREEMENT

In connection with the Services and/or Software being provided to the Partner ("**Partner**", "**Data Controller**") by BRS GOLF Limited and/or GOLFNOW, LLC (as applicable) ("**GOLF**", "**Data Processor**") under an Agreement subject to the GOLF Terms and Conditions ("**Existing Agreement**"), the terms of this Data Processing Agreement ("**DPA**") shall govern the the processing of Partner Data by GOLF as a data processor.

Unless otherwise agreed and except where the contrary intention is obvious, if there is any conflict between the terms of this DPA and any Existing Agreement, this DPA shall take precedence.

1.1 DEFINITIONS

"**Partner Data**" means any Personal Data that relates to the Partner's member and visitor Golfers, provided to GOLF in relation to GOLF's provision of the Software and/or Services, as may be further detailed in the Existing Agreement and/or any applicable Order Forms.

"**Personal Data**" means any information that relates to an individual person and that, alone or in combination with other data, can be used to identify, contact, or precisely locate an individual person, or other information that constitutes "personal data" under applicable Data Protection Law.

"**Data Protection Legislation**" all laws relating to the processing of personal data, privacy and security, including, without limitation, the UK Data Protection Act 1998, the UK GDPR, the EU General Data Protection Regulation 2016/679, the EU Privacy and Electronic Communications Directive 2002/58/EC, as implemented in each jurisdiction, and all amendments, or all other applicable or replacement international, regional, federal or national data protection laws.

Terms such as "**data controller**", "**data processor**", "**personal data**" and "**personal data breach**" shall have the meanings (or reasonable equivalents) ascribed to them in the applicable Data Protection Legislation.

1.2 APPOINTMENT AND INSTRUCTIONS

Partner hereby instructs GOLF to process Partner Data in accordance with this DPA and as required to provide the Services and/or Software.

1.3 PROCESSING OVERVIEW

The categories of Partner Data to be processed by GOLF, the processing activities to be performed under this Agreement, and the subcontractors and processing locations that have been approved by Partner are set out in Schedule 1 (Processing Overview).

1.4 DATA PROCESSOR OBLIGATIONS

GOLF shall:

1.4.1 Only process Partner Data in accordance with Partner's reasonable, lawful and documented instructions given from time to time, including in the Existing Agreement, this DPA and any applicable Order Forms;

1.4.2 ensure its personnel who may be required by GOLF to assist it in meeting its obligations under the Agreement are under a binding obligation to protect the confidentiality of Partner Data;

1.4.3 implement and maintain appropriate technical and organisational measures to protect Client Personal Data, including the measures described in Schedule 2 to this DPA, which may be revised by GOLF from time to time in its sole discretion, and including, as appropriate: (i) the pseudonymisation and encryption of Client Personal Data; (ii) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Client Personal Data in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly

testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;

1.4.4 taking into account the nature of the processing, provide Partner with reasonable assistance and co-operation, insofar as this is possible, to assist the Partner in complying with its obligations under Data Protection Legislation with respect to a Partner Data breach, individual rights requests from Golfers, and otherwise as required by Data Protection Legislation;

1.4.5 provide Partner with such information as is necessary to demonstrate compliance with this DPA and, where required by applicable Data Protection Legislation, allow Partner to audit GOLF's processing of personal data (the terms of which to be agreed by the parties);

1.4.6 subcontract processing of personal data only pursuant to a written agreement that shall impose obligations no less onerous than those set out in this DPA and shall remain liable for the actions of its Sub-Processors. Partner acknowledges and agrees that GOLF may engage the Sub-Processors listed in the Processing Overview / Appendix 1 to the C2P SCC. Partner may reasonably object to GOLF using a new Sub-Processor by notifying GOLF promptly in writing within ten (10) days after receipt of GOLF's notice to be provided by email. In the event Partner objects to a new sub-processor, as permitted in this Condition 1.4.6, GOLF will use reasonable efforts to make available to Partner a change in the Services or recommend a commercially reasonable change to Partner's configuration or use of the Services to avoid processing of Partner Data by the objected-to new Sub-processor. If GOLF is unable to make available such a change within a reasonable period of time, which shall not exceed thirty (30) days, Partner may terminate the applicable Order Form(s) with respect only to those Services that cannot be provided by GOLF without the use of the objected-to new Sub-Processor by providing written notice to GOLF;

1.4.7 adopt reasonable measures to ensure legally compliant cross-border transfers of Partner Data pursuant to this Agreement. Where the provision of the Services and/or Software involves the transfer (including onward transfers) of personal data from the EEA, Switzerland or the United Kingdom to a sub-processor established in a third country that does not ensure an adequate level of protection as defined by applicable Data Protection Legislation, Partner authorises Golf to enter into the controller-to-processor Standard Contractual Clauses ("**C2P SCC**") (as set out at: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en) approved by the European Commission with any such sub-processor on Partner's behalf;

1.4.8 notify Partner without undue delay of any personal data breach, including any accidental, unlawful or unauthorised destruction, disclosure, loss, alteration or access in relation to Partner Data processed on behalf of Partner;

1.4.9 upon termination or expiry of the Agreement, at Partner's choice, promptly delete, return or transfer to Partner's successor all Partner Data in accordance with Conditions 8.4 and 8.5.

1.5 INTERNATIONAL DATA TRANSFERS

If and to the extent GOLF's provision of the Software and/or Services involves the transfer of personal data from a Partner established in the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to GOLF in the United States, the unchanged C2P SCC shall be deemed to be incorporated by reference in this Agreement. Unless otherwise agreed by the parties, where applicable, Schedules 1 and 2 of this DPA shall apply and be deemed to be Appendices 1 and 2 of the C2P SCCs. Nothing in this Agreement shall be construed to prevail over any conflicting clause of the C2P SCCs. Each party acknowledges that it has had the opportunity to review the C2P SCCs. In relation to services provided by GOLF for the benefit of a Partner established in Switzerland, the C2P SCCs will be deemed to be modified to include the corresponding Swiss law references and the terms of such modified C2P SCCs will be incorporated by reference into this DPA. If requested, GOLF will promptly execute a standalone C2P SCC agreement with the Partner in Switzerland.

1.6 PARTNER WARRANTIES

Partner warrants that its collection and processing of Partner Data (including the sharing with GOLF under this DPA) shall comply with applicable Data Protection Legislation and that its instructions to GOLF shall be lawful.

SCHEDULE 1

Processing Overview / Appendix 1 to the SCC (processors)

A: Processing Overview and Duration:

B: Informaiton for Appendix 1 of the C2P SCC:

DATA EXPORTER

Data Exporter is the legal entity identified as "Partner" established within the European Union, the European Economic Area (EEA) or one of their member states, the United Kingdom or Switzerland that has purchased Services and/or Software under the Agreement and any applicable Order Forms.

DATA IMPORTER

GOLFNOW, LLC (**GOLFNOW**), established in the United States, is a provider of tee time booking, marketing, technology and management software and services, which processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement.

In the event that the United Kingdom ceases to be a member of the European Union or the European Economic Area, a further Data Importer shall be BRS Golf Limited (**BRS GOLF**), established in the United Kingdom, a provider of tee time booking, marketing, technology and management software and services, which processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement.

1. DATA SUBJECTS

The personal data transferred concern the following categories of data subjects:

Partner's Golfers

2. CATEGORIES OF DATA

The personal data transferred concern the following categories of data:

i. Identification and contact data, including first and last name, user name, email address, date of birth, phone number, mobile phone number, address, town, postcode, country, customer number, club ID and other club details
ii. Transaction / booking data, including booking ID, tee time and date, booking time and date, other booking details, including names of other players
iii. Marketing preferences
iv. IT Information, including IP Address

3. SPECIAL CATEGORIES OF DATA / SENSITIVE PERSONAL DATA (IF APPROPRIATE)

None.

4. PROCESSING OPERATIONS

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

In order to provide the Software and/or Services, GOLF will host, maintain and support a system holding Partner Data. GOLF will grant Partner's Golfers electronic access to this system.

C. PROCESSING LOCATION AND SUB-PROCESSORS

The Sub-Processors GOLF engages vary depending on the Software and Services the Partner receives and the country where they are located.

SUBPROCESSOR	LOCATION	SUB-PROCESSOR ROLE	WEBSITE
Amazon	United Kingdom Ireland United States Australia	Data centre hosting facility	https://aws.amazon.com/
Google (Cloud)	Belgium United Kingdom Australia	Server hosting facility	https://cloud.google.com/
NICE InContact	United Kingdom United States	Cloud-based contact center platform / partner support - incontact	https://www.niceincontact.com/
Mandrill by MailChimp	United States	Email delivery platform	https://www.mandrill.com/
Paypal	United States	Auto payments/renewals processing	https://www.paypal.com/
Rackspace	United Kingdom United States	Server hosting facility	https://www.rackspace.com/
Salesforce	United States	Cloud-based customer service management and communications service	https://www.salesforce.com/
Vindicia	United States	Subscription billing and recurring payment platform	https://www.vindicia.com/
Clickatell	United States South Africa	SMS messaging platform	https://www.clickatell.com/
Twilio	United States	SMS messaging platform	https://www.twilio.com/
UKDedicated	United Kingdom	Data centre hosting facility	https://www.ukdedicated.com/
Sparkpost	United States	Email delivery service	https://www.sparkpost.com/
Cloudflare	United States	Content delivery network	https://www.cloudflare.com/
Akamai	United States	Content delivery network	https://www.akamai.com/
Highwinds	United States	Content delivery network	https://www.highwinds.com/
Stripe	United Kingdom Ireland Australia United States	Payment processing services	https://stripe.com/

SCHEDULE 2

Appendix 2 to the C2P SCCs - Technical and Organizational Measures

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

This Appendix 2 forms part of the Clauses and must be completed by the parties.

Data importer agrees and warrants that it has implemented and will maintain technical and organisational measures appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. These measures ensure a level of security appropriate to the risks presented by the processing and the nature, scope, context and purposes of the processing, having regard to the state of the art and the cost of their implementation, including as appropriate: (i) the pseudonymisation and encryption of personal data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The measures data importer has taken include, as appropriate and without limitation:

1. Implementation of and compliance with a written information security program consistent with established industry standards and including administrative, technical, and physical safeguards appropriate to the nature of personal data and designed to protect such information from: unauthorized access, destruction, use, modification, or disclosure; unauthorized access to or use that could result in substantial harm or inconvenience to the data exporter, its customers or employees; and any anticipated threats or hazards to the confidentiality, security, availability or integrity of such information.

2. Adopting and implementing appropriate policies and standards related to security;

3. Assigning responsibility for information security management;

4. Devoting adequate personnel resources to information security;

5. Carrying out verification checks on permanent staff who will have access to personal data;

6. Conducting appropriate background checks and requiring employees, vendors and others with access to the personal data to enter into written confidentiality agreements;

7. Conducting training to make employees and others with access to personal data aware of information security risks and to enhance compliance with data importer's policies and standards related to data protection;

8. Preventing unauthorized access to the personal data through the use, as appropriate, of physical and logical (passwords) entry controls, secure areas for data processing, procedures for monitoring the use of data processing facilities, built-in system audit trails, use of secure passwords, network intrusion detection technology, encryption and authentication technology, secure log-on procedures, and virus protection, monitoring compliance with data importer's policies and standards related to data protection on an ongoing basis. In particular, data importer has implemented and complies with, as appropriate and without limitation:

    a. Confidentiality

        (1) Physical access control measures to prevent unauthorized access to data processing systems (e.g., access ID cards, card readers, desk officers, alarm systems, motion detectors, burglar alarms, video surveillance and exterior security);

        (2) Denial-of-use control measures to prevent unauthorized use of data protection systems (e.g., automatically enforced password complexity and change requirements, firewalls, etc.);

        (3) Requirements-driven authorization scheme and access rights, and monitoring and logging of system access to ensure that persons entitled to use a data processing system have access only to the data to which they

have a right of access, and that personal data cannot be read, copied, modified or removed without authorization (virtual access controls);

b. Integrity

(1) Data transmission control measures to ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission, transport or storage on data media, and transfer and receipt of records. In particular, data importer's information security program shall be designed (transfer control):

i. To encrypt in storage any data sets in data importer's possession, including sensitive personal data.

ii. To ensure that any sensitive personal data transmitted electronically (other than by facsimile) to a person outside data importer's IT system or transmitted over a wireless network is encrypted to protect the security of the transmission.

(2) Data Entry control measures to ensure data importer can check and establish whether and by whom personal data has been input into data processing systems, modified, or removed (input control);

c. Availability and resilience

Availability control includes measures to ensure that personal data are protected against accidental destruction and loss.

d. A process for regularly testing, assessing and evaluating

(1) Organizational control

(2) Privacy by default

(3) Subcontractor supervision measures to ensure that, in the case data importer is permitted to use sub-processors, the data is processed strictly in accordance with the controller's instructions including, as appropriate and without limitation;

i. Measures to ensure that personal data is protected from accidental destruction or loss including, as appropriate and without limitation, data backup, retention and secure destruction policies; secure offsite storage of data sufficient for disaster recovery; uninterrupted power supply, and disaster recovery programs;

ii. Measures to ensure that data collected for different purposes can be processed separately including, as appropriate and without limitation, physical or adequate logical separation of client data.

9. Taking such other steps as may be appropriate under the circumstances.