sodexo
QUALITY OF LIFE SERVICES

EMPLOYEE & CONSUMER ENGAGEMENT | Bringing people and business together

GDPR DATA PROCESSING TERMS & CONDITIONS

BRS UK Version 2.0

RECTIALS

(1) Sodexo Motivation Solutions U.K Limited, a company registered in England with Company Number 02680629 of registered office, One Southampton Row, London, WC1B 5HA, United Kingdom **(''Sodexo'')** acts as sole Controller in relation to the Personal Data.

(2) The supplier or service provider **(''Supplier'')** acts as a Processor and processes Personal Data on behalf of Sodexo.

Background

(A) The parties have entered into an agreement or arrangement directly or on behalf of **(Main Agreement)** for the Supplier to supply services to Sodexo or Sodexo's customer.

(B) The provisions set forth below apply where the Supplier processes Personal Data for the purposes of performing the Services or in connection with the provision of the Services.

1 DEFINITIONS

Controller: any natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. For the purposes of this Agreement, Sodexo is the Controller.

Data Protection Regulation: up to but excluding 25 May 2018, the Data Protection Act 1998 and thereafter (i) unless and until the GDPR is no longer directly applicable in the UK, the GDPR and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK and then (ii) any successor legislation to the GDPR or the Data Protection Act 1998.

Data Subject: any identified or identifiable natural person from whom Personal Data is collected.

General Data Protection Regulation or GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27th, 2016 on the protection of natural persons with regard to the processing of Personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Personal Data: any data that is considered as personal data under the Data Protection Regulation, specifically information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal Data Breach or Breach: any suspected or actual security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

Processing or Processed: every operation or set of operations which is performed with regard to Personal data, including without limitation the collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, combining, linking to other data, blocking, erasure or destruction of Personal Data.

Processor: any natural or legal person, public authority, agency or other body which processes Personal Data on behalf of a Controller. For the purposes of this Agreement, the Supplier is the Processor.

Services: any services to be provided by Supplier to Sodexo or Sodexo's customer or an individual of a client's under the Main Agreement or arrangement.

Subprocessor: any natural or legal person engaged by the Supplier only for the performance of Processing under this Agreement and as specifically authorised in advance in writing by Sodexo.

Third Party(/ies): any company or entity other than Sodexo, the Supplier, Data Subjects and persons who, under the direct authority of Sodexo or the Supplier are authorised to process Personal Data. Subprocessor(s) are not considered as a Third Party.

Third-Party Country: any country, territory or specified sector within that country, outside of the European Union (EU) and the European Economic Area (EEA).

2 STATUS OF THIS AGREEMENT

2.1 This Agreement (including attached appendixes) supplements and is incorporated into the Main Agreement.

2.2 If there is an inconsistency between any of the provisions of this Agreement and the provisions of the Main Agreement, the provisions of this Agreement shall prevail as between the parties.

2.3 The consideration for this Agreement consists of the mutual obligations and benefits between the parties set out in the provisions below.

3 COMPLIANCE WITH DATA PROTECTION REGULATION

3.1 Both parties will comply with all applicable requirements of the Data Protection Regulation.

4 STATUS OF THE PARTIES

4.1 Sodexo acts as sole Controller in relation to the Personal Data.

4.2 If Sodexo requires the Supplier to Process Personal Data, it will transfer the relevant Personal Data to the Supplier who will act as Processor for this purpose.

5 OBLIGATIONS OF THE SUPPLIER

The Supplier shall:

5.1 comply with the Data Protection Regulation in relation to its performance of the Processing, in such a way as to not expose Sodexo to any violation of the Data Protection Regulation;

5.2 process Personal Data as a Processor on behalf of and only in accordance with the instructions of Sodexo (which may be specific instructions or instructions of a general nature and which may be supplemented from time to time by further instructions) and only for the purposes of performing the Agreement and determined by Sodexo;

5.3 promptly comply with any Sodexo request or instruction requiring the Supplier to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing;

5.4 promptly inform Sodexo if the Supplier cannot provide such compliance for whatever reason of its inability to comply, in which case Sodexo reserves the right to immediately and automatically suspend any Processing;

5.5 not modify, amend or alter the contents of the Personal Data unless the Supplier has the prior written consent of Sodexo;

5.6 upon Sodexo's request, assist Sodexo in the fulfilment of Sodexo's obligations to provide Data Subjects with any information required by law or by this Agreement, to respond to requests and complaints made by the Data Subjects, to put in place appropriate security measures, to notify Personal Data Breach to the supervisory authority and/or to Data Subjects if required, and to carry out a

data protection impact assessment or to prior consult the supervisory authority where required;

5.7 notify Sodexo immediately if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Regulation;

5.8 maintain a record of all categories of Processing activities carried out on behalf of Sodexo in the performance of this Agreement;

5.9 notify Sodexo in writing (by sending an email at the following email address: br.uk.gdpr.legal@sodexo.com) regarding any request received directly from a Data Subject and not later than 48 hours after receiving such a request and shall provide reasonable assistance to the Data Subject in order to respond to such Data Subject request;

5.10 promptly inform Sodexo (if lawful to do so) in writing (by sending an email to br.uk.gdpr.legal@sodexo.com) if it receives any correspondence or request for information from a supervisory authority in relation to the Personal Data to which this Agreement relates; (ii) not later than 48 hours after receiving such a correspondence or request, shall provide such reasonable assistance to the Data Subject in order to respond to such supervisory authority; and (iii) provide assistance and co-operation by supporting Sodexo to carry out any required risk assessments and audits of the Supplier's Data Processing operations; and

5.11 delete or return all the Personal Data and any copies thereof which it is processing, has processed or have had processed on behalf of the Controller in format agreed upon with Sodexo after the end of the performance of the Agreement at the choice of Sodexo, and delete existing copies unless the applicable local law requires storage of the Personal Data.

6 SECURITY AND CONFIDENTIALITY MEASURES

6.1 The Supplier shall take and implement the appropriate technical and organisational security and confidentiality measures to ensure the security and confidentiality of the Personal Data, and regularly update them, to ensure a level of security appropriate to the risk related to the Processing of the Personal Data and to protect such data from any unauthorised or unlawful Processing, accidental loss, alteration, destruction or damage, as may be required or directed by Sodexo from time to time.

6.2 The Supplier must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

(a) The pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) 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

(d) a process for regularly testing, assessing and evaluating the effectiveness of security measures.

6.3 During the term of this Agreement, the Supplier shall implement and maintain up to date a training and awareness program for its employees and Subprocessors regarding Personal Data security. The Supplier shall ensure that the authorised persons are properly trained in the Processing of Personal Data and only have access to the Personal Data on a need-to-know basis subject to obligation of confidentiality. The Processor shall also take steps to ensure that the authorised persons do not process the Personal Data except on instructions from Sodexo, unless the Supplier is required to do so by European Union or Member State law.

6.4 The Supplier shall require that any of its employees and Subprocessors entrusted with Processing Personal Data:

(a) have undertaken to comply with the principle of confidentiality, are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data;

(b) have undertaken training on the Data Protection Regulation relating to handling Personal Data and how it applies to their particular duties; and

(c) are aware both of the Supplier's duties and their personal duties and obligations under the Data Protection Regulation and this Agreement.

7 SUBPROCESSORS

The Supplier shall not disclose or permit the disclosure of Personal Data to any Third Party, and/or shall not subcontract whole or part of the Processing to any Third Party, unless the Supplier has the prior written consent of Sodexo as required by applicable Member State law or law of the European Union. Where the Supplier is authorised by Sodexo to subcontract whole or part of the Processing, the Supplier shall enter into a contract with the Subprocessor whereby the Supplier shall require the Subprocessor to comply with obligations no less onerous than the Supplier's obligations under this Clause. In particular, the Subprocessor shall provide sufficient guarantees to implement appropriate technical and organizational security and confidentiality measures. Such subprocessing shall not release the Supplier from its responsibility for its obligations under this Agreement. The Supplier shall be responsible for the work and activities of such Subprocessors, and the Supplier shall be held liable for the acts and omissions of any Subprocessor(s) to the same extent as if the acts or omissions were performed by the Supplier.

8 INTERNATIONAL PERSONAL DATA TRANSFERS

8.1 The Supplier will not process Personal Data in any Third-Party Country and/or have Personal Data processed in any Third-Party Country (including a Subprocessor), including for onward transfers of Personal Data from a Third-Party Country to another Third-Party Country, in any manner whatsoever, unless the Supplier has the specific prior written consent of Sodexo.

8.2 In particular, the Supplier will not host nor subcontract the hosting of Personal Data in a Third-Party Country without Sodexo's consent.

8.3 Where such specific prior written approval has been granted, the Supplier shall:

8.3.1 execute, with Sodexo, the Standard Contractual Clauses for the transfer of Personal Data between Controllers and Processors as set out in the European Commission decision of February 5, 2010 (C (2010) 593) (hereafter the ''Standard Contractual Clauses'') as may be amended from time to time; the Supplier shall comply with the data importer's obligations set out in the Standard Contractual Clauses and Sodexo will comply with the data exporter's obligations as

laid down in the said Standard Contractual Clauses;

8.3.2 if previously and specifically agreed in writing with Sodexo, implement alternative means to the Standard Contractual Clauses in order to ensure an adequate level of protection of Personal Data for the purpose of the Data Protection Regulation; and

8.3.3 warrant that any duly authorised Subprocessor processing Personal Data in any Third-Party Country shall comply with the same obligations as set forth in this clause 8.3; the Supplier shall justify that its duly authorised Subprocessor comply with the said same obligations upon Sodexo's first request.

9 PERSONAL DATA BREACH

9.1 In the event of a Personal Data Breach arising during the Processing of the Personal Data by the Supplier, the Supplier shall, at its own cost:

9.1.1 notify Sodexo in writing (by sending an email to (br.uk.gdpr.legal@sodexo.com) about the Personal Data Breach within 72 hours of becoming aware of it, and provide information about:

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

(b) the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) the likely consequences of the Breach; and

(d) the measures taken or proposed to be taken to address the Breach including, where appropriate, measures to mitigate its possible adverse effects.

9.1.2 after investigating the causes of such a Personal Data Breach, take such actions as may be necessary or reasonably expected by Sodexo to minimise the effects of any Breach;

9.1.3 take all actions as may be required by Data Protection Regulation and more generally provide Sodexo with reasonable assistance in relation to Sodexo's obligations to notify the Breach to the supervisory authority and to the Data Subjects as the case may be;

9.1.4 maintain any record of all information relating to the breach, including the results of its own investigations and authorities' investigations;

9.1.5 cooperate with Sodexo and take all measures as necessary to prevent future Breach from occurring again; and

9.1.6 where Sodexo determines that a Breach notification is required under Data Protection Regulation, the Supplier shall reimburse Sodexo for all reasonable costs associated with providing notification to Data Subjects and supervisory authorities, unless the Supplier demonstrates that the Breach was caused by Sodexo's negligence or wilful misconduct.

9.2 The Supplier will not inform any Third Party or Data Subject of any Personal Data Breach without first obtaining Sodexo's prior written consent, except when required to do so by law.

9.3 The Supplier agrees that Sodexo has the sole right to determine:

(a) whether to provide notice of the Personal Data Breach to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or others, as required by law or regulation or in Sodexo's discretion, including the contents and delivery method of the notice; an

(b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

10 EVIDENCE AND AUDIT RIGHTS

10.1 The Supplier shall provide, upon request of Sodexo, all information necessary to demonstrate compliance with the obligations laid down in this Agreement.

10.2 The Supplier will:

(a) conduct an information security audit before it first begins processing any Personal Data and repeat that audit as reasonably required by Sodexo;

(b) produce a written report that includes detailed plans to remedy any security deficiencies identified by the audit;

(c) provide Sodexo with a copy of the written audit report; and

(d) remedy any deficiencies identified by the audit within 14 days.

10.3 Upon reasonable notice to the Supplier, Sodexo may audit the Supplier's compliance with the Supplier's obligations under this Agreement or with any applicable data protection law or regulation. The Supplier will allow for, contribute to and help Sodexo (or a third party mandated by Sodexo) with the aforementioned audit. The Supplier will give Sodexo (or a third party mandated by Sodexo) access to its facilities, offices, and any information necessary to Sodexo to evaluate the Supplier's compliance.

10.4 resume delivery and performance of the Goods and Services in accordance with this Agreement, and in particular any Quality Standards after which Sodexo shall cease to exercise any rights pursuant to this Clause in respect of the rights of step-in.

11 LIABILITY AND INDEMNIFICATION

The Supplier shall be held liable in any event of any breach of its obligations under this Agreement and/or non-compliance with the Data Protection Regulation. The Supplier shall indemnify Sodexo against all costs, claims, damages or expenses incurred by Sodexo arising out of any breach of the Supplier's obligations under this Agreement or the Supplier's non-compliance with the Data Protection Regulation, without being subject to any limitation of liability set forth in the Main Agreement.

12 TERM AND TERMINATION

12.1 This Agreement will remain in full force and effect so long as:

(a) the Main Agreement remains in effect, or

(b) the Supplier retains any Personal Data related to the Main Agreement in its possession or control.

12.2 Any provision of this Agreement that expressly or by implication should come into or continue in force on or after termination of the Main Agreement in order to protect Personal Data will remain in full force and effect.

12.3 The Supplier's failure to comply with the terms of this Agreement is a material breach of the Main Agreement. In such event, Sodexo may terminate any part of the Main Agreement authorising the processing of Personal Data effective immediately on written notice to the Supplier without further liability or obligation.

13 JURISDICTION AND APPLICABLE LAW

This Agreement shall be governed by and interpreted in accordance with English law and the parties agree to submit to the non-exclusive jurisdiction of the English Courts.