Microtill Limited

NuvolaPOS Data Processing Agreement

1. INFORMATION ABOUT THIS DPA

1.1 This data processing agreement ("DPA") forms part of the Agreement between Microtill Limited, a company registered in England and Wales with company number 06454630, whose registered office is at New Centaur House, 11-19 Hamberts Road, South Woodham Ferrers, Essex CM3 5UF (the "Supplier"), and the customer named in the Agreement (the "Customer"), and sets out the terms that apply to the processing of Personal Data in connection with the provision and receipt of the Services.

1.2 Capitalised terms used but not defined in this DPA shall have the meaning given to them in the Agreement.

2. DEFINITIONS AND INTERPRETATION

2.1 In this DPA the following terms shall have the following meanings unless the context requires otherwise:

Term	Meaning
"Agreement"	means the agreement between the Supplier and the Customer for the provision of the Services, comprising the Supplier's EPoS Service Contract or other written terms for NuvolaPOS signed or accepted by the Customer, any order form or quotation accepted under them, this DPA and any document referred to in the same.
"Applicable Law"	means any law, regulation or binding requirement of a Supervisory Authority or court of competent jurisdiction that applies to a Party, including Data Protection Laws.
"Business Day"	means a day other than a Saturday, Sunday or public holiday in England, and "Business Days" shall be construed accordingly.
"Business Hours"	means 9.00 am to 5.30 pm on a Business Day.
"Controller"	has the meaning given to it by GDPR.
"Customer Data"	means all data, including Personal Data, entered into or generated through the Services by or on behalf of the Customer, its staff or its guests and customers.
"Data Protection Laws"	means, in relation to any Personal Data which is Processed in the performance of this Agreement: (i) in respect of the United Kingdom, the Data Protection Act 2018, the UK GDPR and the Data (Use and Access) Act 2025; and (ii) in respect of the European Economic Area, the EU GDPR, in each case together with any national implementing laws, regulations, secondary legislation and any other applicable or equivalent data protection or privacy laws, as amended or updated from time to time, and any successor legislation to such laws.
"Data Subject"	has the meaning given to it by GDPR.
"GDPR"	means the UK GDPR and/or the EU GDPR, in each case as applicable, where: (a) "UK GDPR" means Regulation (EU) 2016/679 General Data Protection Regulation as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of Section 3 of the European Union (Withdrawal) Act 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019; and (b) "EU GDPR" means Regulation (EU) 2016/679 General Data Protection Regulation as applicable in the European Economic Area, together with any applicable national data protection legislation of the relevant EEA member state.
"Personal Data"	has the meaning given to it by GDPR, and except for the caveat at Clause 4, relates only to personal data, or any part of such personal data, of which the Customer is the Controller and in relation to which the Supplier is the Processor in providing the Services under this Agreement.
"Personal Data Breach"	has the meaning given to it by GDPR.
"Process" and **"Processing"**	have the meaning given to it by GDPR.

Term	Meaning
"Processor"	has the meaning given to it by GDPR.
"Services"	means the NuvolaPOS point of sale, table reservation and related hosted services, and the associated support, provided by the Supplier to the Customer under the Agreement.
"Special Categories of Personal Data"	means those categories of data listed in Article 9(1) GDPR.
"Supervisory Authority"	means any regulatory authority responsible for the enforcement of Data Protection Laws, which shall at least include, in respect of the UK, the UK Information Commissioner's Office and, in respect of the EEA, the relevant competent supervisory authority of the applicable member state.

2.2 In this DPA, references to "Clauses" are to clauses of this DPA and references to "Annex A" are to the annex to this DPA. Headings do not affect interpretation, words in the singular include the plural and vice versa, and "including" means including without limitation. If there is any conflict between this DPA and any other part of the Agreement in relation to the Processing of Personal Data, this DPA shall prevail, except in relation to liability, which is governed by Clause 9.

3. ROLES OF THE PARTIES

3.1 The Parties acknowledge that, to the extent the Supplier is acting as a Controller in relation to Personal Data as set out in Clause 4, the Supplier acts as a separate and independent Controller from the Customer.

3.2 Except as in the limited circumstances provided for in Clause 4, the Parties acknowledge that:

3.2.1 for the purposes of Data Protection Laws, the Customer is the Controller and the Supplier is the Processor of any Personal Data; and

3.2.2 the Personal Data shall be in respect of data shared by necessity by the Customer with the Supplier for the provision and receipt of the Services only.

3.3 Card payments taken through the Services are processed by the Customer's own card payment provider under the Customer's merchant agreement. That provider acts as an independent Controller in relation to card payment data and is not a Subprocessor of the Supplier.

4. SUPPLIER ACTING AS CONTROLLER

4.1 To the extent the Supplier is acting as Controller, the Supplier shall:

4.1.1 comply with Data Protection Laws when Processing Personal Data;

4.1.2 only Process Personal Data:

4.1.2.1 in order to perform the Supplier's obligations under this Agreement; and

4.1.2.2 solely to the extent permitted by Applicable Laws to the extent necessary for the following purposes as Controller:

4.1.2.2.1 maintaining and developing the Supplier's relationship with the Customer;

4.1.2.2.2 billing and invoicing;

4.1.2.2.3 compliance with quality control and risk management procedures;

4.1.2.2.4 IT security-related processing (for example, automated scanning of incoming and outgoing emails for viruses);

4.1.2.2.5 complying with legal and regulatory obligations; and

4.1.2.2.6 establishing, exercising and defending legal claims;

4.1.3 notify the Customer as soon as reasonably practicable upon becoming aware of a Personal Data Breach affecting Personal Data, and, where reasonably practicable, provide a copy of any proposed notification and consider in good faith any comments made by the Customer before notifying the Personal Data Breach to any Supervisory Authority; and

4.1.4 comply with Data Protection Laws in relation to any transfers of Personal Data under GDPR that would otherwise be prohibited but for the implementation of appropriate safeguards in accordance with Article 46 GDPR.

5. PROCESSING DETAILS AND INSTRUCTIONS

5.1 The scope, nature and purpose of the Processing, which constitutes the Customer's Processing instruction as Controller to the Supplier as Processor, is set out in Annex A.

5.2 The Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws. The Supplier shall inform the Customer immediately if, in the Supplier's opinion, an instruction from the Customer violates Data Protection Laws.

5.3 Each Party confirms that, in the performance of this Agreement, it shall comply with Data Protection Laws.

5.4 The Services include free-text fields, including the optional "Notes" field on the online booking form, in which guests or the Customer's staff may enter allergy, dietary, accessibility or similar information. Such information may be Special Categories of Personal Data (for example health data, or data that reveals religious belief). As Controller, the Customer is responsible for identifying a condition for Processing under Article 9 GDPR (usually explicit consent), for providing privacy information to Data Subjects, and for deciding whether a data protection impact assessment is required. The Supplier shall protect such data in accordance with the technical and organisational measures in Clause 6.3 and shall not use it for any purpose other than providing the Services.

6. SUPPLIER OBLIGATIONS AS PROCESSOR

The Supplier shall:

6.1 Process Personal Data only on documented instructions from the Customer, unless required to do so by Data Protection Laws or any other Applicable Law to which the Supplier is subject; in such a case, the Supplier shall inform the Customer of that legal requirement before Processing, unless that Applicable Law prohibits the Supplier to so inform the Customer;

6.2 take reasonable steps to ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality undertakings;

6.3 ensure that the Supplier has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of the Supplier's systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by the Supplier);

6.4 be generally authorised to engage another Processor to Process Personal Data (**"Subprocessor"**), subject to the Supplier:

6.4.1 making available to the Customer a list of Subprocessors authorised to Process Personal Data (**"Subprocessor List"**), the initial Subprocessor List as at the date of this DPA being set out in Annex A;

6.4.2 notifying the Customer of any intended changes to its use of Subprocessors by providing the Customer with notice of any updates to the Subprocessor List, which the Supplier shall provide to the Customer at least 30 (thirty) calendar days prior to authorising any new Subprocessor;

6.4.3 including terms in its contract with each Subprocessor which are no less protective than those set out in this Agreement;

6.4.4 remaining liable to the Customer for any failure by each Subprocessor to fulfil its obligations in relation to the Processing of the Customer's Personal Data.

6.5 allow the Customer, in relation to any notice received under Clause 6.4.2, a period of 14 (fourteen) calendar days from the date of the notice to register any reasonable objection to the use of that Subprocessor. Where any objection is registered, the following shall apply:

6.5.1 the Parties shall meet as soon as possible to discuss the reasons for the objection, whereby the Customer shall provide the Supplier with all details of the concerns which led to the objection;

6.5.2 if the Customer does not withdraw the Customer's objection within one (1) month from the date on which the Customer made the Customer's objection, the Supplier will use reasonable efforts to make available to the Customer a change in the Services or recommend a commercially reasonable change to the Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Subprocessor without unreasonably burdening the Customer;

6.5.3 if the Supplier is unable to make available to the Customer a change in the Services or recommend a commercially reasonable change to the Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Subprocessor as per Clause 6.5.2 above, or if the Customer does not accept the proposed changes or recommendations, the Supplier shall not proceed with appointing that Subprocessor;

6.5.4 if the Supplier's provision of Services is not possible without engaging the proposed Subprocessor, the Supplier shall be entitled to proceed with appointing that Subprocessor. The Supplier shall notify the Customer that the appointment of that Subprocessor is required in order for the Supplier to provide the Services and the Customer may terminate the Agreement by providing written notice within 30 days from receipt of the Supplier's notice under this Clause 6.5.4.

6.6 taking into account the nature of the Supplier's Processing, assist the Customer by putting in place appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the Data Subject's rights laid down in Data Protection Laws, to the extent that such requests relate to Personal Data Processed in connection with this Agreement;

6.7 Notwithstanding Clause 6.6 above, the Supplier shall direct:

6.7.1 all individual Data Subject requests, complaints or other communications (whether from the Data Subject or on their behalf); and

6.7.2 any requests, correspondence or communications from a Supervisory Authority,

to the Customer within two (2) Business Days of receipt and provide all reasonable co-operation to allow the Customer to investigate any such request and to fulfil the Customer's obligations under applicable Data Protection Laws. The Supplier shall not engage with such Data Subject, requester or Supervisory Authority directly;

6.8 assist the Customer, at the Customer's cost, in responding to any request from a Data Subject and in ensuring compliance with the Customer's obligations under Data Protection Laws with respect to Personal Data Breach notifications, data protection impact assessments and consultations with Supervisory Authorities;

6.9 in relation to the Customer's assessment of the Supplier's compliance with this DPA:

6.9.1 at the Customer's request, make available to the Customer all information necessary to demonstrate the Supplier's compliance with this DPA (which obligation may be satisfied by providing relevant certifications (such as ISO/IEC 27001 or equivalent), third-party audit reports or other appropriate documentation);

6.9.2 to the extent that information obtained pursuant to Clause 6.9.1 is insufficient for the Customer to verify the Supplier's compliance with this DPA and Data Protection Laws, the Customer shall be entitled to carry out an inspection of the technical and organisational measures taken by the Supplier as relevant to the Supplier's compliance with this DPA upon giving at least 30 (thirty) calendar days prior notice, unless a shorter period is required (in particular in cases where a Supervisory Authority requires an inspection to be performed at shorter notice), provided that any inspection takes place during normal Business Hours and with no unreasonable disruption to the Supplier's business, is proportionate to the Services the Supplier provided to the Customer and the criticality or importance of such Services, adheres to commonly accepted national and international audit standards, is conducted no more than once in any calendar year (unless a Supervisory Authority requires otherwise), does not include access to systems, data or information relating to any other customer of the Supplier, and employees or third-party auditors being subject to appropriate confidentiality obligations in relation to any audit and / or inspection, and the costs of any such audit or inspection being borne by the Customer;

6.9.3 where the Customer requires additional assistance or information beyond what is reasonably necessary to demonstrate the Supplier's compliance with this DPA, the Supplier may charge reasonable fees for providing such additional assistance or information on a time and materials basis;

6.10 notify the Customer promptly and without undue delay if the Supplier becomes aware of a Personal Data Breach relating to the Supplier's obligations under this Agreement, which notification shall include, where available:

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

6.10.2 the likely consequences of the Personal Data Breach; and

6.10.3 the measures taken or proposed to be taken to address and mitigate the Personal Data Breach;

6.11 in relation to any such notification under Clause 6.10, take all reasonable measures to prevent any further negative impact of the Personal Data Breach. The Supplier shall provide assistance, and provide the Customer with sufficient information so that the Customer is able to meet any obligations to assess and report a Personal Data Breach under the Data Protection Laws, which may be provided in stages as it becomes available to the Supplier, including obtaining any information that needs to be included in a notification to the Supervisory Authority or impacted Data Subjects; and

6.12 not transfer any Personal Data outside of the United Kingdom and the European Economic Area unless the Customer's prior written consent has been obtained (such consent not being required in respect of transfers of Personal Data to Subprocessors appointed in accordance with Clause 6.4) and appropriate safeguards have been implemented in accordance with Article 46 GDPR, which safeguards may include the Standard Contractual Clauses approved by the European Commission or any other lawful transfer mechanism recognised under Data Protection Laws (and the Customer authorises the Supplier to enter into such transfer mechanisms with Subprocessors on the Customer's behalf where required).

7. DATA RETURN AND DESTRUCTION

7.1 Upon termination or expiry of the Agreement, the Customer may, within thirty (30) days, request the return or export of Personal Data Processed by the Supplier on the Customer's behalf. Following the expiry of that period, the Supplier shall delete or irreversibly anonymise all Personal Data, unless Applicable Law requires retention of such Personal Data.

7.2 Notwithstanding Clause 7.1, Personal Data may be retained in backups, archives or disaster recovery systems until such data is deleted in accordance with the Supplier's standard retention cycles. During this period, such Personal Data shall remain protected in accordance with this DPA and shall not be actively Processed.

7.3 Upon written request, the Supplier shall confirm that deletion has been completed in accordance with this Clause 7, to the extent technically feasible.

7.4 The Customer is responsible for ensuring that it has securely exported or otherwise retained any Personal Data it requires prior to deletion. The Supplier shall not be liable for any loss of Personal Data following deletion carried out in accordance with this Clause 7.

8. INDEMNITY

The Customer agrees to indemnify the Supplier, and keep the Supplier indemnified, and defend the Supplier at the Customer's own expense, against all costs, claims, damages or expenses incurred by the Supplier or for which the Supplier may become liable, due to any failure by the Customer or the Customer's employees or agents to comply with this DPA.

9. LIABILITY

Nothing in this DPA shall increase or extend either Party's liability beyond that set out in the Agreement.

Signed for and on behalf of the Parties:

	Microtill Limited	
	(Supplier)	**(Customer)**
Signature	_____	_____
Name	_____	_____
Position	_____	_____
Date	_____	_____

ANNEX A

Personal Data processing purposes and details

Subject matter of Processing	Processing of Personal Data as necessary for the Supplier to provide the Services under the Agreement.
Duration of Processing	For the duration of the Agreement and any applicable retention period in accordance with Clause 7.
Nature of Processing	Processing activities may include collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, transmission, restriction, deletion or destruction of Personal Data.
Purpose of Processing	Provision and operation of the Services, including: (a) hosting and storage of Personal Data; (b) Processing of Customer Data to run the Customer's point of sale, orders, customer accounts, loyalty and staff records; (c) taking and managing table reservations made online or by the Customer's staff, and sending booking confirmation and reminder emails on the Customer's behalf; (d) support, maintenance and troubleshooting; (e) security monitoring and fraud prevention; and (f) analytics and performance monitoring (in aggregated and anonymised form where possible).
Personal Data Categories	Depending on the Customer's use of the Services, Personal Data may include: (a) guest and customer details: name, email address, telephone number and, where entered, address; (b) reservation details: booking date and time, party size, table or area, booking status and attendance (including no-shows), and notes; (c) order, purchase and loyalty history linked to a customer account; (d) staff details: name, login and PIN credentials, role and permissions, and clock-in and clock-out times; (e) technical data (e.g. IP address, device information, log data); and (f) Special Categories of Personal Data: allergy, dietary, accessibility or similar information that guests or staff may enter in free-text fields, including the optional "Notes" field on the online booking form (see Clause 5.4).
Data Subject Types	(a) the Customer's employees, workers and contractors who use the Services; (b) the Customer's guests and customers, including people who make reservations, place orders or hold loyalty or customer accounts; and (c) any other individuals whose Personal Data is included in Customer Data.

Approved Subprocessors (initial Subprocessor List)

Name of Subprocessor	Processing activities	Location	Safeguard mechanism
Amazon Web Services EMEA SARL (Amazon Web Services)	Hosting of the Services, databases, backups, and sending of booking emails	United Kingdom (London, eu-west-2)	No restricted transfer; AWS data processing addendum
TeamViewer Germany GmbH	Remote access to the Customer's tills for support and maintenance, during which Customer Data may be displayed on screen	Germany (EEA)	UK adequacy regulations (EEA); TeamViewer data processing agreement; sessions end-to-end encrypted