Version 2.4 July 2023

DATA PROCESSING AGREEMENT (DPA)

This DPA is a Schedule to the Software as a Service Agreement (SaaS Agreement) accepted by the Customer. The Customer is the Data Controller with respect to this DPA. POS ONE is the Data Processor with respect to this DPA.

1. DEFINITIONS

Data Controller means the 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; in this DPA it is the Customer

Data Processor means a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller; in this DPA it is POS ONE

Data Protection Law means, as binding on either Party or the Services: a) the GDPR; b) any laws that implement any such laws; and c) any laws that replace, extend, re-enact, consolidate, or amend any of the foregoing

Data Subject means an identified or identifiable natural person

DPA means this Data Protection Agreement

GDPR means the General Data Protection Regulation (EU) 2016/679

International Organization means an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

Personal Data means any information relating to an identified or identifiable natural person ('data subject'); 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 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

Processing has the meaning given in applicable Data Protection Laws from time to time (and related expressions, including process, processed, processing, and processes shall be construed accordingly)

Protected Data means Personal Data received from or on behalf of the Data Controller in connection with the performance of the Data Processor's obligations under this DPA

Sub-Processor means any agent, subcontractor, or other third party (excluding its employees) engaged by the Data Processor for carrying out any processing activities on behalf of the Data Controller in respect of the Protected Data.

2. DATA PROCESSOR'S COMPLIANCE WITH DATA PROTECTION LAWS

The parties agree that the Data Controller is a Controller and that the Data Processor is a Processor for the purposes of processing Protected Data pursuant to this DPA. The Data Processor shall at all times comply with the applicable Data Protection Laws in connection with the processing of Protected Data. The Data Controller shall ensure all instructions given by it to the Data Processor in respect of Protected Data (including the terms of this DPA) shall at all times be in accordance with the applicable Data Protection Laws.

3. DATA PROCESSOR'S COMPLIANCE WITH DATA PROTECTION LAWS

The Data Processor shall process Protected Data in compliance with the obligations placed on it under Data Protection Laws and the terms of this DPA.

4. INSTRUCTIONS

4.1 The Data Processor shall only process the Protected Data in accordance with Annex A of this DPA (and not otherwise unless alternative processing instructions are agreed between the parties in writing) except where otherwise required by applicable law (and shall inform Data Controller of that legal requirement before processing, unless applicable law prevents it doing so on important grounds of public interest).

4.2 Without prejudice to section 2 of this DPA, if the Data Processor believes that any instruction received by it from the Data Controller is likely to infringe the Data Protection Laws, it shall promptly inform the Data Controller and be entitled to cease to provide the relevant Services until the parties have agreed appropriate amended instructions which are not infringing.

5. SECURITY

5.1 In accordance with the Data Protection Laws, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of the processing of the Protected Data to be carried out under or in connection with this DPA, as well as the risks of varying likelihood and severity for the rights and

freedoms of natural persons and the risks that are presented by the processing, especially from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the Protected Data transmitted, stored or otherwise processed, the Distributor shall implement appropriate technical and organizational security measures appropriate to the risk, including as appropriate those matters mentioned in Articles 32(a) to 32(d) (inclusive) of the GDPR.

6. SUB-PROCESSING AND PERSONNEL

6.1 The Data Processor shall:

6.1.1 not permit any processing of Protected Data by any agent, subcontractor, or another third party (except its or its Sub-Processors' own employees in the course of their employment that are subject to an enforceable obligation of confidence with regards to the Protected Data) without the written authorization of Data Controller

6.1.2 prior to the relevant Sub-Processor carrying out any processing activities in respect of the Protected Data, appoint each Sub-Processor under a written contract containing materially the same obligations as under this DPA, including an obligation to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR, that is enforceable by the Data Processor and ensure each such Sub-Processor complies with all such obligations

6.1.3 remain fully liable to the Data Controller under this DPA for all the acts and omissions of each Sub-Processor as if they were its own

6.1.4 ensure that all persons authorized by the Data Processor or any Sub-Processor to process Protected Data are subject to a binding written contractual obligation to keep the Protected Data confidential.

6.2 Data Controller authorizes the appointment of the Sub-Processors listed at the website of POS ONE: Sub-processors.

7. ASSISTANCE

7.1 The Data Processor shall:

7.1.1 implement the appropriate technical and organizational security measures with due regard for the current state of the art, the cost of their implementation, and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, pursuant to Article 32 of the GDPR

7.1.2 notify of any personal data breach to the supervisory authority to the relevant supervisory authority pursuant to Article 33 of the GDPR, as well as communication of any personal data breach to the data subject, pursuant to Article 34 of the GDPR.

7.1.3 prepare any impact assessment, pursuant to Article 35 of the GDPR

7.1.4 consult with the relevant supervisory authority, pursuant to Article 36 of the GDPR.

7.2 The Data Processor shall (at the Data Controller's cost) taking into account the nature of the processing, assist Data Controller (by appropriate technical and organizational measures), insofar as this is possible, for the fulfillment of the Data Controller's obligations to respond to requests for exercising the Data Subjects' rights under Chapter III of the GDPR (and any similar obligations under applicable Data Protection Laws) in respect of any Protected Data including requests for access, rectification, blocking or deletion. The Data Processor must also assist the controller by implementing appropriate technical and organizational measures for the fulfillment of the Data Controller's obligation to respond to such requests.

8. CONFIDENTIALITY

8.1 The Data Processor shall keep the Protected Data confidential.

8.2 The Data Processor shall not disclose the Protected Data to third parties or take copies of the Protected Data unless strictly necessary for the performance of the Data Processor's obligations towards the Data Controller according to the DPA, and on condition that whoever the Protected Data is disclosed to is familiar with the confidential nature of the Protected Data and has accepted to keep the personal data confidential in accordance with this DPA.

8.3 All terms of the DPA apply to any of the Data Processor's employees, and the Data Processor must ensure that its employees comply with the DPA.

8.4 The Data Processor must limit access to the Protected Data to employees for whom access to said Protected Data is necessary to fulfill the Data Processor's obligations towards the Data Controller.

8.5 The obligations of the Data Processor under this section 9 persist without time limitation and regardless of whether the cooperation of the Parties has been terminated.

8.6 The Data Controller shall treat confidential information received from the Data Processor confidentially and may not unlawfully use or disclose the confidential information.

9. INTERNATIONAL TRANSFERS

The Data Processor shall not process and/or transfer, or otherwise directly or indirectly disclose, any Protected Data in or to countries outside the European Union or to any international

organization without the prior written consent of the Data Controller.

10. AUDITS AND PROCESSING

The Data Processor shall, in accordance with Data Protection Laws, make available to the Data Controller such information that is in its possession or control as is necessary to demonstrate the Data Processor's compliance with the obligations placed on it under this DPA and to demonstrate compliance with the obligations on each party imposed by Article 28 of the GDPR (and under any equivalent Data Protection Laws equivalent to that Article 28), and allow for and contribute to audits, including inspections, by Data Controller (or another auditor mandated by Data Controller) for this purpose (subject to a maximum of one audit request in any 12 month period under this clause 12).

11. BREACH

The Data Processor shall notify Data Controller without undue delay and in writing on becoming aware of any Personal Data Breach in respect of any Protected Data.

12. DELETION/RETURN AND SURVIVAL

On the end of the provision of the Services relating to the processing of Protected Data, at the Data Controller's cost and Data Controller's option, the Data Processor shall either return all of the Protected Data to the Data Controller or securely dispose of the Protected Data (and thereafter promptly delete all existing copies of it) except to the extent that any applicable law requires the Data Processor to store such Protected Data. This Schedule shall survive the termination or expiry of this DPA following the earlier termination or expiry of this DPA in the case of all other paragraphs and provisions of this Schedule.

13. AMENDMENTS AND ASSIGNMENTS

13.1 The Parties may at any time agree to amend this DPA. Amendments must be in writing.

13.2 The Data Processor may not assign or transfer any of its rights or obligations arising from this DPA without the Data Controller's prior written consent.

14. COMMENCEMENT AND TERMINATION

14.1 This DPA shall enter into force on the Data Controller's acceptance of the SaaS Agreement.

14.2 The DPA may be renegotiated by both parties if changes in law or disagreements in the DPA give rise to this.

14.3 This DPA is valid for the duration of the processing of the Protected Data. Regardless of the termination of the underlying contractual DPA of the Parties, the Data Processing DPA will remain in force until the termination of the processing and the deletion of the data by the Data Processor and any authorized Sub-Processors.

15. INDEMNIFICATION AND LIABILITY

15.1 Data Controller shall indemnify and keep indemnified the Data Processor against all losses, claims, damages, liabilities, fines, sanctions, interest, penalties, costs, charges, expenses, compensation paid to Data Subjects, demands and legal and other professional costs (calculated on a full indemnity basis and in each case whether or not arising from any investigation by, or imposed by, a supervisory authority) arising out of or in connection with any breach by Data Controller of its obligations under this Schedule.

15.2 Limitation of Liability and Indemnification Claims. The liability of the Data Processor under this DPA is, to the widest possible extent, limited in accordance with the limitation of liability agreed in the DPA.

15.3 Fines issued by the Supervisory Authority. The Parties agree that the general principle of division of liability between the Parties relating to fines imposed by any relevant Supervisory Authority is based on that the respective party has to fulfill its obligations under the GDPR and the Act and that any fines imposed by a Supervisory Authority should be paid ultimately by the party which has materially failed in its performance of its legal obligations under the GDPR or the Act. Consequently, the Data Processor shall at its own costs give the Data Controller all information and assistance available required to respond to such claims.

15.4 The Data Processor shall review the requirements and instructions issued by the Data Controller regarding data processing activities performed by the Data Processor under this DPA on their behalf and notify the Data Controller beforehand in writing if it believes that implementation of such requirements or instructions would likely constitute a violation of the GDPR or the Data Protection Regulation applicable to the Data Processor. The Data Processor shall, in its written notice, advise the Data Controller on how such requirements and instructions should be amended to avoid such potential violation of the GDPR or the Act by the Data Processor due to following such requirements or instructions. If the Data Controller, in its written response, continues requiring that the Data Processor shall implement such requirements and instructions despite the associated risks, then the Data Controller shall at their own cost indemnify and hold the Data Processor harmless against any fines imposed by any Supervisory Authority.

ANNEX A: DATA PROCESSING AND SECURITY DETAILS

Processing of the Protected Data by the Data Processor under this DPA shall be for the subject matter, duration, nature, and purposes and involve the types of Personal Data and categories of Data Subjects set out in this Annex A.

1. SUBJECT MATTER OF PROCESSING:

The Data Processor will have access to the Personal Data of the Customer, the Named Users of the Customer, and the specific information that the Customer adds to the POS ONE Service to store the Personal Data and ensure the POS ONE Service's availability, integrity, and confidentiality, as well as to provide remote services to the Customer's users of the POS ONE Service.

2. DURATION OF THE PROCESSING:

The Data Processor may process the Personal Data for as long as the Data Controller subscribes to the Service as defined in the SaaS Agreement.

The Data Processor may delete the Personal Data upon termination of the Service and shall delete the Personal Data no later than 12 months after the termination unless the Data Processor is required to retain the Personal Data for a longer period of time according to legal requirements.

3. NATURE AND PURPOSE OF THE PROCESSING:

The Data Processor shall process data, including Personal Data, to perform the Service described in the SaaS Agreement and on www.posone365.com.

4. TYPE OF PERSONAL DATA:

Name, address, email, telephone numbers, and invoice identification numbers.

5. CATEGORIES OF DATA SUBJECTS:

Customers, suppliers, and employees of the Data Controller.

6. SPECIFIC PROCESSING INSTRUCTIONS:

The Service is automated, and processing will only take place upon command of the Data Controller. Support services by the Data Controller will only take place upon specific request by the relevant person at the Data Controller.

7. SUB-PROCESSORS:

The current and updated list of Sub-processors may be found here: Sub-processors.