PRIVACY POLICY OF

BETTERPOS SP. Z O.O. WITH REGISTERED OFFICE IN MYSŁOWICE

§ 1.

1. This Privacy Policy (hereinafter referred to as **the Policy**) is a document describing the method of processing personal data and the obligations of the Controller in relation to the processing of personal data.

2. The Controller is BetterPOS with its registered office in Mysłowice (41 - 400) at ul. Obrzeżna Północna 16, entered into the Register of Entrepreneurs of the National Court Register maintained by Katowice-Wschód District Court in Katowice, 8th Commercial Division of the National Court Register, under KRS number 0000764774, NIP: 382173032, share capital: PLN 5000 (hereinafter referred to as **the Controller**).

3. The Policy is updated on an ongoing basis, at least once a year.

§ 2.

1. The Controller conducts business activity consisting of renting POS terminal devices and providing appropriate software for them, inter alia.

2. The Controller processes personal data in accordance with the requirements provided for, in particular, in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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 (General Data Protection Regulation) and the Act of 10 May 2018 on the protection of personal data, to the extent indicated in the information clause available on the website

§ 3.

1. The Controller applies technical and organisational measures to ensure the adequate level of security of the processed personal data, in particular:

    a. only persons authorised by the Controller who have submitted a declaration to keep the data and the method of securing it confidential are allowed to process the personal data. The obligation to submit the declaration does not apply to persons obliged to keep professional secrecy,

    b. maintains the register of authorised persons and stores the content of the declarations referred to in Art. 3, point 1a,

    c. regularly trains the personnel having access to personal data and improves their knowledge regarding personal data security,

    d. protects documents and electronic devices against access by unauthorised persons, including through data encryption,

    e. may keep the register of processing operations.

2. The Controller may appoint the Data Protection Officer. In the event of appointment of the Officer the Controller:

    a. supports the Data Protection Officer in fulfilling the tasks entrusted to him/her by providing him/her with the resources necessary to perform those tasks and with access to personal data and processing operations, as well as the resources necessary to maintain his/her expertise,

    b. ensures the Data Protection Officer's independence in performing his/her functions, including: by not giving instructions on how to perform his/her tasks.
3. The Controller may use the services of external entities to support the Controller in its day-to-day activities, in particular, in the field of IT, accounting and marketing services. In this case, the Controller:

a. uses the services only of such entities that ensure an adequate level of security of personal data and the compliance of data processing with the law,
b. concludes with such an entity an entrustment agreement for the processing of personal data,
c. does not transfer personal data to entities outside the European Union.

§ 4.

1. The duties of the personnel allowed to process personal data include:

   a. becoming familiar with and following the legal provisions on personal data protection,

   b. protection of personal data against unauthorised access, modification or destruction,

   c. destroying in a secure manner any media containing personal data,

   d. using IT resources and electronic equipment in a manner consistent with their intended use and in a secure manner, including, but not limited to, changing passwords periodically, keeping the logins and passwords confidential, using device encryption and not leaving equipment unattended; the use of personal equipment may only take place with the prior express consent of the Controller,
   e. notifying immediately the superiors or the Data Protection Officer of any observed irregularities that may affect the security of the processed personal data and of any incidents that breach security,

   f. keeping documentation containing personal data in designated places, with limited access to third parties, especially documents containing sensitive data,

   g. not leaving reception desks unattended.
2. The personnel is responsible for the proper performance of their duties and has been instructed by the Controller on the sanctions resulting from irregularities in this respect, including criminal liability.

§ 5.

1. The Controller stores the documentation provided by Clients for the duration of the service, unless otherwise stated in the concluded contract.

2. The transfer of documents in paper form should take place based on a hand-over protocol. The transfer of documents in digital form should take place in a secure manner, using end-to-end encryption, unless the Client agrees to another form of communication.

§ 6.

1. The Policy enters into force on 25 May 2018 and replaces previous regulations concerning personal data.

2. A template of the authorisation to process personal data constitutes an Appendix to this Policy.