DATA PROCESSING AGREEMENT

QuickPay ApS

Table of contents

Table of contents....1
§ 1 Parties....1
§ 2 Background....2
§ 3 Purpose....2
§ 4 Obligations of the Data Processor....2
§ 5 Transfer of data to other data procesors or third parties....4
§ 6 Amendments....5
§ 7 Breach....5
§ 8 Effective date, duration of processing and termination....5
§ 9 Governing law and jurisdiction....5
§ 10 Signatures....5

§ 1 Parties

Your company:

_____

_____

_____

(the "Data Controller")

and

Quickpay ApS
Company No: DK-21822434
Ostergade 25, **1** tv.
8000 Arhus C
Denmark
(the "Data Processor")

(collectively the "Parties" and individually the "Party")

have concluded this Data Processing Agreement (the "Agreement") on the Data Processor's processing of personal data on behalf of the Data Controller.

§ 2 Background

The personal data to be processed by the Data Processor concerns the data The Data Controller are sending to the Data Processor when selling products on the Internet (making transactions).

§ 3 Purpose

The Data Processor shall only process personal data for purposes which are necessary in order to perform the Services ("the Services") stipulated in the nature of the PSP-product.

§ 4 Obligations of the Data Processor

To the extent that the provision of the Services by the Data Processor involves the processing of personal data within the meaning of the applicable data protection legislation, the Data Processor agrees that:

- The Data Processor warrants to the Data Controller that it complies and will comply with its obligations as a data processor under the applicable data protection legislation.

- All processing by the Data Processor of the personal data provided by the Data Controller shall only be carried out on documented instructions from the Data Controller for the provision of the Services, including with regard to transfers of personal data in any form or by any means whatsoever outside its usual place of business, unless the Data Processor is required to do so by applicable Union or Member State Law. In such case, the Data Processor shall inform the Controller of that legal requirement immediately before processing the personal data, unless applicable legislation prohibits such information on important grounds of public interest. Furthermore, the Data Processor is obliged to comply with any and all data protection legislation in force from time to time, and to inform the Data Controller immediately if, in his opinion, an instruction may breach any applicable data protection provisions.

- The Data Processor shall implement and follow all appropriate and necessary technical and organizational security measures, including any additional measures, required to ensure a level of security appropriate to the harm that might result from unauthorised or unlawful access, processing or accidental loss, destruction or damage to the personal data, and shall ensure that the data is not accidentally or unlawfully destroyed, lost or impaired or brought to the knowledge of unauthorized third parties, abused or otherwise processed in a manner which is contrary to the applicable Danish personal data protection legislation, or any other applicable data protection regulation that may be in force from time to time. In any case and unless otherwise directed in writing by the Data Controller, the Data Processor must, among other things:

    - introduce login and password procedures and set up and maintain a firewall.
    - ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data.
    - ensure that it has the ability to restore the availability and access to the personal data in a timely manner in the event of a physical or technical incident.
    - implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

    - ensure the pseudonymisation and encryption of personal data when appropriate.
    - ensure that only employees with a work related purpose have access to the personal data, and ensure that all employees with access to the data shall not process the data except on instructions from the Data Controller, unless he or she is required to do so by Union or Member State Law.
    - store data storage media securely so that it is not accessible to third parties.
    - ensure that buildings and systems used for data processing are secure and that only high-quality hardware and software, which is regularly updated is used.
    - ensure that tests and waste material are destroyed in accordance with data protection requirements on the specific written instruction of the Data Controller. In particular cases, to be determined by the Data Controller, such tests and waste material must be stored or returned.

- The personal data are confidential in nature and shall be kept confidential. The Data Processor shall ensure that all employees and/or agents engaged in processing the personal data have received proper training, adequate instructions and guidelines on the processing of the personal data, and have committed themselves to confidentiality. In addition, the Data Processor must ensure that the employees involved with the processing of the personal data are familiar with the applicable and implemented security requirements and will keep the personal data confident.

- If the Data Processor processes personal data in another EU/EEA member state other than Denmark, the Data Processor must also comply with any and all legislation concerning security measures in that member state.

- The Data Processor must notify the Data Controller immediately where there is an interruption in operation, a suspicion that data protection rules have been breached or other irregularities in connection with the processing of the personal data occur. In any case, the Data Processor shall (and shall procure that its agents shall) promptly notify the Data Controller of any security incident that leads or may lead to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed by the Data Processor in connection with the Services ("Security Breach"). The notification to the Data Controller shall in any case include: (a) the nature of the Security Breach; (b) the recommended measures to minimize the negative effects of the Security Breach; (c) the identified and probable consequences of the Security Breach on the processing of personal data by the Data Processor in connection with the Services; and (d) the (proposed) actions (to be) taken to remedy the consequences for the protection of personal data processed by the Data Processor in connection with the Services.

- The Data Processor shall (and shall procure that its agents shall) provide full cooperation to the Data Controller with respect to any Security Breach, including - but not limited to - providing adequate information and support relating to (a) the recovery of the Security Breach and the prevention of future Security Breaches; (b) the limitation of the impact of the Security Breach on the privacy of the data subjects involved; (c) the

compensation of damages suffered by the Data Controller as a result of the Security Breach.

- Upon the request of the Data Controller, the Data Processor must promptly provide the Data Controller with all information necessary to demonstrate that the Data Processor has taken the necessary technical and organizational security measures, and to demonstrate compliance with any and all applicable data protection regulations. In this connection, the Data Processor shall allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller. The Data Controller must, in addition hereto, compensate the Data Processor for time spent by it and its employees in connection with the above.

- The Data Processor shall promptly notify the Data Controller about any legally binding request for disclosure of the personal data by law enforcement or other applicable authority unless otherwise prohibited by applicable law.

- Upon request of the Data Controller, the Data Processor shall assist the Data Controller in taking any actions deemed necessary or appropriate to deal with complaints or allegations of or in connection with a failure to comply with the appli-cable data protection legislation.

§ 5 Transfer of data to other data procesors or third parties

The Data Processor may only transfer the personal data processed by the Data Processor in connection with the Services to other data processors or third parties in circumstances where it has received specific, prior written authorisation from the Data Controller to this effect. The Data Processor is not entitled to disclose or hand over personal data to third parties or other data processors without the prior written instruction of the Data Controller, unless such disclosure or handover is stipulated by applicable law.

Before transferring personal data to another data processor (sub-processor), the Data Processor must ensure that (1) the Data Controller approved the engagement of such sub-processor as set out in clause 5.1, (2) the Data Processor and the sub-processor enter into an agreement on similar terms to those set out in this Agreement, especially with respect to providing sufficient guarantees to implement appropriate technical and organizational security measures ("Sub-Data Processor Agreement"); (3) the Sub-Data Processor Agreement terminates automatically upon termination of this Agreement; and (4) the Sub-Data Processor Agreement must be submitted to and approved by the Data Controller.

Where that sub-processor fails to fulfil its obligations, the Data Processor shall remain fully liable to the Data Controller for the performance of that other sub-processor's obligations.

§ 6 Amendments

In the event of amendments to the Danish data protection legislation, the Data Controller is entitled to amend the instructions set out in this Agreement on the giving of 2 (two) weeks' written notice when forwarding the new written instructions to the Data Processor. The Data Processor must however, at all times, comply with the applicable legislation on the protection of personal data.

§ 7 Breach

The Data Processor shall indemnify the Data Controller against any claims, costs (including reasonable expenses for legal services), loss, liability, expenses or damages incurred by the Data Controller as a result of the Data Processor's breach of this Agreement.

§ 8 Effective date, duration of processing and termination

This Agreement becomes effective on the date of signing hereof.

Termination of the separately concluded Master Agreement will result in the termination of this Agreement. However, the Data Processor remains subject to the obligations stipulated in this Agreement, as long as the Data Processor processes personal data on behalf of the Data Controller, i.e. until the personal data have been returned to the Data Controller and deleted or destroyed.

In the event of the termination of the Agreement, the Data Controller is entitled to determine the media format to be used by the Data Processor when returning the personal data and to determine if the personal data should instead be deleted or destroyed. Upon first request of the Data Controller, the Data Processor shall comply with any instructions of the Data Controller with respect to such deletion or destruction of the personal data.

§ 9 Governing law and jurisdiction

This Agreement is governed by Danish law.

Any claim or dispute arising from or in connection with this Agreement must be settled by a competent court of first instance in Aarhus Denmark.

§ 10 Signatures

Date:…….....……..……	Date:21.11.2017.....……..……
…….....	…….....
For the Data Controller	For the Data Processor, QuickPay