# Data Processing Agreement

Merchant (the "Data Controller")

and

DIBS (the "Data Processor")

(separately referred to as a “Party” and collectively the “Parties”)

have concluded this

**DATA PROCESSING AGREEMENT**
(the "Agreement")

regarding the Data Processor's processing of personal data on behalf of the Data Controller.

## 1. The processed personal data

1.1 This Agreement has been entered into together with, and forms an integral part of, the agreement on payment gateway services entered into between the Parties (the “Main Agreement”).

1.2 The Data Processor processes the personal data which is part of the transaction data processed by the Data Processor on behalf of the Data Controller. The data subjects on which personal data is processed on behalf of the Data Controller by the Data Processor are payment service users.

1.3 The Data Processor may initiate processing of personal data on behalf of the Data Controller after the Main Agreement enters into force. The processing has the duration of 2 years from the date the personal data is obtained by the Data Processor.

1.4 The Agreement and the Main Agreement are interdependent and this Agreement can only be terminated if the Main Agreement is correctly terminated.

## 2. Purpose

2.1 The Data Processor must only process personal data for purposes set forth in the Main Agreement.

## 3. Obligations of the Data Controller

3.1 The Data Controller warrants that the personal data is processed for legitimate and objective purposes and that the Data Processor is not processing more personal data than required for fulfilling such purposes.

3.2 The Data Controller is responsible for ensuring that a valid legal basis for processing exists at the time of transferring the personal data to the Data Processor. Upon the Data Processor's request, the Data Controller undertakes, in writing, to account for and/or provide documentation of the basis for processing.

3.3 In addition, the Data Controller warrants that the data subjects to which the personal data pertains have been provided with sufficient information on the processing of their personal data.

## 4. Obligations of the Data Processor

4.1 All processing by the Data Processor of the personal data provided by the Data Controller must be in accordance with instructions set forth in this Agreement (including with regard to data transfers) and which constitute the Data Controllers complete and final instructions to the Data Processor, unless i) EU or EU Member State law to which the Data Processor is subject requires other processing of the personal data by the Data Processor, or ii) in the event the Data Processors makes changes to its systems, processes, etc. which requires changes to the instructions, in which case Data Processor will notify the Data Controller of amendents to the instructions in the same manner as the Data Processor provides notice of Amendments to the General Terms and Conditions under the Main Agreement.

4.2 Should the Data Controller in its reasonable opinion believe, and be able to substantiate, that the amendments to the instructions introduced by the Data Processor cause the Data Controller to be non-compliant with General Data Protection Regulation, the Data Controller shall be entitled to terminate this Agreement and the Main Agreement by giving notice of termination to the Data Processor within the 10 business days from receiving notice of the amendments, otherwise the amendments will be deemed accepted by the Data Controller and will effectively become part of this Agreement.

4.3 The Data Processor must immediately inform the Data Controller if, in the Data Processor’s opinion, an instruction infringes the EU General Data Protection Regulation or the data protection provisions of a Member State.

4.4 The Data Processor must take all necessary technical and organisational security measures, including any additional measures, required to ensure that the personal data specified in clause 1.2 is not accidentally or unlawfully destroyed, lost or impaired or brought to the knowledge of unauthorised third parties, abused or otherwise processed in a manner which is contrary to applicable national law in the relevant EU/EEA member states in force at any time. These measures shall meet and be equivalent to the certificate and security requirements specified by card associations and the authorities, including the PCI DSS (Payment Card Industry – Data Security Standard), for details see https://www.pcisecuritystandards.org.

The security measures deemed necessary and applied by the Data Processor shall be risk based, and will be updated from time to time by the Data Processor.

4.5 The Data Processor must ensure that employees authorized to process the personal data have committed themselves to confidentiality or are under appropriate statutory obligation of confidentiality.

4.6 If so requested by the Data Controller, the Data Processor must state and/or document that the Data Processor complies with the requirements of the applicable data protection legislation, including documentation regarding the data flows of the Data Processor as well as procedures/policies for processing of personal data. In terms of documentation supporting such statement of compliance, it is agreed that the Data Processors Attestation of Compliance with the Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS) is sufficient.

4.7 Taking into account the nature of the processing, the Data Processor must, as far as possible, assist the controller by appropriate technical and organisational measures, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the data subject's rights as laid down in chapter 3 in the General Data Protection Regulation.

4.8 The Data Processor, or another data processor (sub-data processor) must send requests and objections from data subjects to the Data Controller, for the Data Controller's further processing thereof, unless the Data Processor is entitled to handle such request itself. If requested by the Data Controller, the Data Processor must assist the Data Controller in answering any such requests and/or objections.

4.9 If the Data Processor processes personal data in another member state, the Data Processor must comply with legislation concerning security measures in that member state.

4.10 The Data Processor must notify the Data Controller where there is a data breach, as defined in 4.12 of the General Data Protection Regulation. The Data Processor's deadline for notifying the Data Controller of a security breach is 24 hours from the moment the Data Processor becomes aware of a security breach. If requested by the Data Controller, the Data Processor must assist the Data Controller in relation to clarifying the scope of the security breach, including preparation of any notification to the competent Data Protection Agency and/or data subjects.

4.11 The Data Processor must make available to the Data Controller all information necessary to demonstrate compliance with article 28 of the General Data Protection Regulation and the Agreement. This requirement can be met by the Data Processor demonstrating a valid PCI compliance certification and/or the relevant and required sections (as determined by the Data Processor) from the latest annual PCI DSS compliance audit performed on the Data Processor. Details regarding the audit procedures and scope are available from the PCI Security Standards Council, https://www.pcisecuritystandards.org, or can be obtained from the Data Processor upon request.

4.12 In addition to the above, the Data Processor must to the extent reasonable assist the Data Controller in ensuring compliance with the Data Controller's obligations under article 32-36 of the General Data Protection Regulation. This assistance will take into account the nature of the processing and the information available to the Data Processor.

## 5. Transfer of data to sub-data processors or third parties

5.1 The Data Processor must comply with the conditions laid down in article 28, paragraph 2 and 4 of the General Data Protection Regulation to engage another data processor (sub-data processor).

This implies that the Data Processor does not engage another data processor (sub-data processor) to performance of the Agreement without prior specific or general written approval from the Data Controller.

5.2 The Data Controller hereby specifically authorizes the Data Processor to engage affiliates of the Data Processor as sub-data processors. Additionally, the Data Controller hereby grants the Data Processor a general power of attorney to enter into agreements with sub-data processors. The Data Processor must inform the Data Controller of any changes concerning the addition or replacements of sub-data processors no later than 30 days prior to a new sub-data processor commencing processing of the personal data. The Data Processor will notify the Data Controller of any new sub-data processor in the same manner as the Data Processor provides notice of Amendments to the General Terms and Conditions under the Main Agreement.The Data Controller can make reasonable and relevant objections against such changes, provided that such objection is received within 20 days from the Data Processor publishing the updated list of sub-data processors. If the Data Processor continues to wish to use a sub-data processor that the Data Controller has objected to, the Parties have the right to terminate the Agreement and the Main Agreement with a shorter notice, cf. 7.2. During this period the Data Controller must not require that the Data Processor do not use the sub-data processor in question.

5.3 The Data Processor must impose the same obligations on the sub-data processor as set out in the Agreement. This is executed through a contract or another legal act under EU law or the law of a Member State. It must be ensured, i.e., that sufficient guarantees are provided from the sub-data processor to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the General Data Protection Regulation (“back-to-back” terms).

5.4 If the sub-data processor fails to fulfil its data protection obligations, the Data Processor remains fully liable to the Data Controller for the performance of the sub-data processor’s obligations.

5.5 Disclosure, transfer and internal use of the Data Controller’s personal data to third countries or international organisations may only take place in accordance with documented instructions from the Data Controller – unless stipulated by EU law or the law of a Member State to which the Data Processor is subject. If so, the Data Processor must notify the Data Controller of this legal requirement before processing, unless the law prohibits such notification for important grounds of public interests.

5.6 If the personal data stipulated in clause 1.2 is transferred to foreign sub-data processors, it must, in the said data processor agreement, be stated that the data protection legislation applicable in the Data Controller's country applies to foreign sub-data processors. Furthermore, if the receiving sub-data processor is established within the EU, it must be stated in the said data processor agreement that the receiving EU country's specific statutory requirements regarding data processors, e.g. concerning demands for notification to national authorities must be complied with.

The Data Processor must, on behalf of the Data Controller, enter into written data processor agreements with sub-data processors within the EU/EEA. As for sub-data processors outside the EU/EEA, the Data Processor must enter into standard agreements in accordance with Commission

Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries ("Standard Contractual Clauses").

5.7 The Data Controller hereby instructs and grants the Data Processor a general power of attorney to enter into Standard Contractual Clauses with sub-data processors outside the EU/EEA on behalf of the Data Controller, and instructs the Data Processor to enter into such Agreements provided that the entering into of such an agreement is subject to a Standard Contractual Clauses as described in Section 5.7 above or subject to an alternative solution (”Alternative solution”) that enables the lawful transfer of personal data to a third country in accordance with Chapter V of the General Data Protection Regulation. If the Data Processor has entered into Standard Contractual Clauses as described in Section 5.7 the above authorization will constitute the Data Processor’s prior written consent to the subcontracting by the Data Controller of the processing of the personal data, if such consent is required under the Standard Contractual Clauses.

5.8 Upon request from the Data Controller, the Data Processor or a third party selected by the Data Processor shall conduct an audit and provide an audit report, regarding a sub-data processors’ compliance with the obligations and requirements in the sub-data processor agreement with the Data Processor. A request for such an audit report may be made by the Data Controller once per year, and shall be both conducted and provided at the Data Controllers expense.

5.9 On the date of entering into of this Agreement, the Data Processor engages the sub-data processors listed on the Data Processors’ website https://www.dibspayment.com/privacy-policy, which are all approved for use by the Data Controller.

## 6. Liability

6.1 The Parties’ liability is governed by the Main Agreement.

6.2 The Parties’ liability in damages under this Agreement is governed by the Main Agreement.

## 7. Effective date and termination

7.1 This Agreement becomes effective at the same time as the Main Agreement.

7.2 In the event of termination of the Main Agreement, this Agreement will also terminate.

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.

In the situation as described under clause 5.2, the parties have the right to terminate the Main Agreement and the Agreement with a notice of 1 (one) month ending at the end of a month.

7.3 Upon termination of the processing services the Data Processor is obliged to, upon request of the Data Controller, delete or return all personal data to the Data Controller, as well as to delete existing copies, unless retention of the personal data is prescribed by EU or national law.

## 8. Governing law and jurisdiction

8.1 Any claim or dispute arising from or in connection with this Agreement must be settled by a competent court of first instance in the same jurisdiction as stated in the Main Agreement.