DATA PROTECTION POLICY

This Data Protection Policy sets out the policy which B2BinPay LIMITED has adopted in order to facilitate compliance with the Data Protection Act 1998 when it establishes and manages customer relationships and executes transactions

CONTENTS

B2BinPay LIMITED

DATA PROTECTION POLICY

1. INTRODUCTION

1.1 This Data Protection Policy (the "Policy") sets out the policy which B2BinPay Limited (referred to as "we" or "us" in this document) has adopted in order to facilitate compliance with the Data Protection Act 1998 (the "DPA") when we establish and manage customer relationships and execute transactions.

1.2 The DPA regulates the "processing" of "personal data". Its definition of "personal data" covers all information relating to identifiable living individuals which is held on computer, in other automatically-process able form or in a manual filing system which is structured so as to facilitate access to information relating to particular individuals. The definition of "processing" covers any conceivable activity in relation to personal data, including collection, analysis, processing in the ordinary sense of the word, storage, disclosure, international transfer and deletion. Information relating to the companies and other "legal" persons does not refer to the processing of the personal data, moreover, the processing of the data of legal persons does not have to be in compliance with the DPA.

1.3 We process personal data in various circumstances and in relation to various categories of individual. This Policy deals specifically with personal data collected in the context of the establishment and management of our customer relationships and the execution of transactions according to the instructions of our customers ("Customer and/or Transaction Management"). It does not, for example, deal with data protection issues which might arise in relation to our HR or direct marketing activities.

1.4 It should be borne in mind that the DPA regulates processing of personal data relating to all individuals, not just relating to customers. Information relating to individual representatives of corporate customers, or to individuals (or individual representatives of corporate bodies) elsewhere in a payment chain – for example, an ultimate payee or an individual representative of an aggregator - is also protected by the DPA.

1.5 The individuals to whom personal data relate, whether customers or otherwise, are known as "data subjects".

1.6 The UK Information Commissioner (the "Commissioner") is responsible for enforcement of the DPA and has published a range of guidance on data protection issues, all of which is available on the Commissioner's website at www.ico.gov.uk.

1.7 Our principal obligations under the DPA include: (i) processing personal data fairly, legitimately, lawfully and proportionately; (ii) informing individuals regarding our processing of their personal data; (iii) abiding by restrictions on the international transfer of personal data; (iv) keeping personal data secure, taking steps to ensure that they are accurate and up-to-date and deleting them when they

are no longer needed; (v) maintaining an appropriate registration with the Commissioner's office; and (vi) responding appropriately when data subjects seek to exercise their statutory rights of the access, correction and objection.

1.8 A copy of this Policy will be supplied to each employee of B2BinPay Limited. The requirements set out in this Policy and the DPA are mandatory unless otherwise stated and must be followed by all our employees and agents. It is the responsibility of each such person to acquaint themselves with the requirements of this Policy and the DPA. Failure to comply with this Policy and the DPA may constitute a serious disciplinary offence and could result in dismissal.

1.9 This Policy is supplementary to our other published policies, including our conduct of business, anti-money laundering and complaints policies.

2. DATA PROTECTION OFFICER

Mr. Sergejs Bergis has been designated as B2BinPay Limited data protection officer (the "Data Protection Officer"). If you have any questions about this Policy or application in particular circumstances, you should consult the Data Protection Officer.

3. FAIR AND PROPORTIONATE PROCESSING

3.1 The DPA requires that all of our processing of personal data should be fair and lawful and should meet one of various specified conditions. In designing and implementing each Customer and/or Transaction Management procedure involving the processing of personal data, we must take these requirements into account and ensure that they are met.

3.2 We expect that our routine processing of personal data for Customer and/or Transaction Management procedure will generally meet the most general of the available conditions, which is known as the "legitimate interests" condition. The legitimate interest's condition will apply, and allow us to process personal data, if both:

3.2.1 A: the processing is necessary for the purposes of legitimate interests that we, or a person to whom we disclose the data, pursue (these may be business, compliance or other purposes); and

3.2.2 B: the processing is not "unwarranted" because it prejudices the rights, freedoms or legitimate interests of the data subjects.

3.3 Each processing operation should, therefore, be assessed to ensure that part A of this condition is met – i.e. we have a legitimate business, compliance or other purpose for carrying out the processing. If part A is met, you should then consider whether the processing will prejudice the data subjects in any way – our expectation is that, provided the other rules in this Policy are followed, our ordinary processing for Customer and/or Transaction Management purposes will not prejudice data subjects' rights, freedoms or legitimate interests. If you consider that there is a potential for prejudice to be caused in a particular case, the prejudice should be balanced against

our interests and a view taken on whether our interests outweigh the prejudice to the data subjects.

3.4 If you are in any doubt as to whether the legitimate interest's condition is met, you should consider whether the processing can be justified on the basis that it meets any of the other statutory conditions available in the DPA. The other conditions most likely to apply are as follows:

3.4.1 Processing is justified if it is necessary to fulfil a UK legal obligation. This will include, for example, processing in order to carry out legally-required anti-money-laundering checks; or in response to a UK court order. Foreign legal requirements are not automatically sufficient to justify disclosure or other processing of personal data.

3.4.2 Processing is justified if it is necessary for the performance of a contract with the data subject or to take steps at the data subject's request with a view to entering into such a contract. This will justify some processing of personal data relating to individual customers.

3.4.3 Processing can be justified on the basis of data subject consent. Our customer contracts should, therefore, include consents to the processing of individual customer data that will be necessary as part of our Customer and/or Transaction Management procedures.

3.5 The requirement that personal data should be processed lawfully can be breached in a number of circumstances, not covered by this Policy because in themselves they fall outside the scope of the DPA – for example, processing for fraudulent purposes would be unlawful and would therefore breach the DPA.

3.6 The DPA also prohibits the processing of excessive, irrelevant or inadequate personal data. Systems and procedures should be designed so as not to collect personal data which are excessive or irrelevant (in particular: personal data should not be collected on a "just-in-case" basis) and, of course, you should ensure that the data collected are adequate for the relevant purposes.

3.7 Personal data collected for any given purpose should not then be used for a purpose which is incompatible with that purpose – we would not expect this to be an issue in the ordinary course of Customer and/or Transaction Management, however.

3.8 We expect the general requirement that processing of personal data should be fair to be met if all the other requirements of this Policy are met.

4. TRANSPARENCY / INFORMATION-PROVISION

4.1 The information to be made available is (a) our identity; (b) the purposes for which we expect to process the data; and (c) any further information that needs to be provided to ensure that our processing of the data is fair.

4.2 We are required under the DPA to ensure that data subjects have various information readily available to them. This requirement is subject to exceptions, however, and these exceptions are of relatively wide application in the context of

Customer and/or Transaction Management. In particular, (a) information only needs to be made available where it is practicable to do so; (b) in the case of personal data which are not collected directly from the data subject (for example, payee data collected from a payer customer), we are not obliged to provide information if to do so would involve disproportionate effort; and (c) we take the view that we can assume that data subjects have, and need not therefore make available, information which should reasonably be obvious to them.

4.3 We must ensure that our customer contracts concluded with our individual customers include the following information:

4.3.1 our identity;

4.3.2 the purposes for which we process their information (including know-your-client and related compliance purposes as well as the execution of Transactions and Customer Management generally); and

4.3.3 the following further information, which, we consider, needs to be provided to ensure that our processing of customer data is fair:

(a) the categories of person to whom we may disclose customer data (including, for example, non-customer payers and payees; aggregators; any persons with whom we might share data for fraud prevention purposes; debt collection agencies; and regulatory and prosecuting authorities);
(b) the fact that, if payments are made to persons outside the European Economic Area, this may involve transfers of the customer's personal data to jurisdictions which do not have data protection laws as strict as those in the UK (see also paragraph 5 below); and
(c) the information as to the customer's rights of access and correction under the DPA (see paragraph), and contact details so that they can contact the Data Protection Officer if they want to exercise those rights.

Our customer contracts should also require customers to pass this information on to any individuals whose personal data they provide to us.

4.4 We take the view that we do not need to provide information to data subjects other than individual customers to justify our processing of their personal data for routine Customer and/or Transaction Management purposes. In particular:

4.4.1 We take the view that the effort involved in contacting an individual noncustomer payer or payee, whose personal data are given to us by a customer, in order to provide him or her with information about our processing of his or her personal data, would be disproportionate given that we process his or her information only in order to facilitate a transaction of which he or she will in any case be aware.

4.4.2 We take the same view in relation to individual representatives of our customers – having required our customers to pass the required information on to their representatives we take the view that the effort involved in contacting the representatives directly would be disproportionate.

5. INTERNATIONAL TRANSFER

5.1 The DPA restricts transfers of personal data to most countries and other territories outside the European Economic Area (the European Union plus Iceland, Liechtenstein and Norway).

5.2 Transfers can be made as necessary to facilitate a transaction, on the basis that they are necessary to perform a contract with the data subject (where the data relate to a customer) or entered into in the interests of the data subject (where they relate to an overseas payee).

5.3 Except for transfers necessary to facilitate a transaction, personal data should not be transferred to countries or territories outside the European Economic Area unless the Data Protection Officer has considered the proposed transfer and concluded, on the basis of legal advice if necessary, that it can be made without breach of the DPA.

6. SECURITY, ACCURACY AND DATA DELETION

6.1 We must have in place appropriate technical and organisational security measures to protect the personal data that we process for Customer and/or Transaction Management purposes against unauthorised or unlawful processing and accidental loss, destruction or damage.

6.2 We need to identify the particular security measures that are "appropriate" in the context of our business. They must deliver a level of security which is appropriate to the nature of the data and the risks associated with unauthorised or unlawful processing and accidental loss, destruction or damage. We must, in particular, take reasonable steps to ensure the reliability of our employees who have access to the data.

6.3 If any aspect of our processing of personal data for Customer and/or Transaction Management purposes is outsourced to a third party service provider, including the outsourcing of any wider function which includes the processing of personal data, we must:

6.3.1 satisfy ourselves that the service provider will have appropriate technical and organisational security measures in place as discussed in paragraphs 6.1 and 6.2;

6.3.2 ensure that the arrangement is governed by a written agreement which requires the service provider to process the data only on our instructions and imposes on the service provider obligations equivalent to our obligations as set out in paragraphs 6.1 and 6.2; and

6.3.3 while the arrangement is in place, take reasonable steps from time to time to ensure that the service provider is meeting its security obligations in practice.

6.4 We must take reasonable steps to ensure that the personal data that we process are accurate and, where relevant, up to date.

6.5 We must delete personal data when we no longer need them, given the purposes for which they are processed. This does not, for example, prevent us from keeping records containing personal data which may be relevant if there is a future dispute with a customer or another person, but it does require us to delete those records when a dispute is no longer a real possibility unless we have another legitimate purpose for continuing to keep the personal data.

7. SENSITIVE PERSONAL DATA

7.1 We do not seek to collect or process personal data identified by the DPA as "sensitive" for Customer and/or Transaction Management purposes. You should not collect or process sensitive personal data for these purposes and should delete them if you become aware that we have collected them, except with the approval of the Data Protection Officer given on the basis of an assessment of the requirements of the DPA.

7.2 The DPA's definition of "sensitive personal data" covers personal data consisting of information as to: racial or ethnic origin; political opinions; religious or other similar beliefs; trade union membership; physical or mental health or condition; sexual life; the commission or alleged commission of any offence; or any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

8. AUTOMATED DECISION-TAKING

8.1 We do not use so-called "automated decision-taking" techniques for Customer and/or Transaction Management purposes. You should not use such techniques except with the approval of the Data Protection Officer given on the basis of an assessment of the requirements of the DPA.

8.2 The DPA's restrictions on the use of automated decision-taking cover systems which make decisions which significantly affect individuals solely on the basis of the automated processing of their personal data, without any human intervention. Examples would be the use of automated credit-scoring tools to pre-screen credit applications and the use of automated tools to pre-screen applications for employment. Semi-automated systems, where the ultimate decision is made or reviewed by a human being, are not caught by these rules.

9. REGISTRATION

9.1 We maintain a registration with the Commissioner's office which covers our processing of personal data for Customer and/or Transaction Management (and other) purposes.

9.2 You should keep the Data Protection Officer aware of material changes to the purposes for which we process personal data or, within any given purpose, the categories of personal data that we process, the categories of data subject to whom the data relate, the categories of person to whom we disclose the data or the countries or territories outside the European Economic Area to which we transfer the data, so that he or she can ensure that the registration is amended accordingly.

10. RIGHTS OF ACCESS, CORRECTION AND OBJECTION

10.1 Data subjects have statutory rights of access to and correction of the personal data that we hold about them. They also have a statutory right to object to our processing of their personal data – that is, to require us to stop processing their data – although only in very limited circumstances.

10.2 If a data subject attempts to exercise any of these statutory rights you should immediately pass his or her communication to the Data Protection Officer so that he or she can ensure that we respond appropriately and within the timescale laid down under the DPA.

10.3 In recording and processing personal data for Customer and/or Transaction Management purposes you should bear in mind data subjects' rights of access. You should not record personal data that you would not want the data subject to see.