

Data Protection Policy **for Customers and Suppliers**

1. OVERVIEW

- 1.1 The Company takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the **Data Protection Act 2018** (the '2018 Act') and the **EU General Data Protection Regulation** ('GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.
- 1.2 This policy applies to customers and suppliers. If you fall into one of these categories then you are a 'data subject' for the purposes of this policy. You should read this policy and any other notice we issue to you from time to time in relation to your data.
- 1.3 The Company has measures in place to protect the security of your data in accordance with our Data Security Policy. A copy of this can be obtained from the Data Protection Team, **BSP International Foundations Ltd, Claydon Business Park, Gipping Road, Great Blakenham, Ipswich, Suffolk IP6 0NL.**
- 1.4 The Company will hold data in accordance with our Data Retention Policy. A copy of this can be obtained from the Data Protection Team, **BSP International Foundations Ltd, Claydon Business Park, Gipping Road, Great Blakenham, Ipswich, Suffolk IP6 0NL.** We will only hold data for as long as necessary for the purposes for which we collected it.
- 1.5 The Company is a '**data controller**' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.
- 1.6 This policy explains how the Company will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the Company.

- 1.7 It is intended that this policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, the Company intends to comply with the 2018 Act and the GDPR.

2. DATA PROTECTION PRINCIPLES

- 2.1 Personal data must be processed in accordance with six '**Data Protection Principles.**' It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

3. HOW WE DEFINE PERSONAL DATA

- 3.1 '**Personal data**' means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.
- 3.2 This policy applies to all personal data whether it is stored electronically, on paper or on other materials.
- 3.3 We may collect your personal data when you provide it to us in a credit account application form or other related documents
- 3.4 We may collect and use the following types of data about you:
- your name and/or business name;

- your name and/or business address
- email address and/or business email address
- your bank account details
- VAT registration number
- credit reference agencies

4. **HOW WE DEFINE PROCESSING**

4.1 **‘Processing’** means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

5. **HOW WILL WE PROCESS YOUR PERSONAL DATA?**

5.1 The Company will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

5.2 We will use your personal data for:

- performing the contract of (or services) between us;
- complying with any legal obligation; or

if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do

not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights in section 10 below.

6. SHARING YOUR PERSONAL DATA

- 6.1 Sometimes we might share your personal data with group companies to carry out our obligations under our contract with you or for our legitimate interests.
- 6.2 We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.
- 6.3 We do not send your personal data outside the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

7. HOW SHOULD YOU PROCESS PERSONAL DATA FOR THE COMPANY?

- 7.1 Everyone who works for, or on behalf of, the Company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Company's Data Security and Data Retention policies.
- 7.2 The Company's Data Protection Officer is responsible for reviewing this policy and updating the Board of Directors on the Company's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.
- 7.3 You should not share personal data informally.
- 7.4 You should keep personal data secure and not share it with unauthorised people.
- 7.5 You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.

- 7.6 You should not make unnecessary copies of personal data and should dispose of any copies securely.
- 7.7 You should use strong passwords.
- 7.8 You should lock your computer screens when not at your desk.
- 7.9 Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.
- 7.10 Do not save personal data to your own personal computers or other devices.
- 7.11 Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Data Protection Officer.
- 7.12 You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.
- 7.13 You should not take personal data away from Company's premises without authorisation from your line manager or Data Protection Officer.
- 7.14 Personal data should be shredded and disposed of securely when you have finished with it.
- 7.15 You should ask for help from our Data Protection Officer if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.
- 7.16 Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.
- 7.17 It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

8. HOW TO DEAL WITH DATA BREACHES

- 8.1 We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights

and freedoms of individuals then we must also notify the Information Commissioner's Office within 72 hours.

- 8.2 If you are aware of a data breach you must contact the Data Protection Team immediately and keep any evidence you have in relation to the breach.

9. **SUBJECT ACCESS REQUESTS**

- 9.1 Data subjects can make a '**subject access request**' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request you should forward it immediately to the Data Protection Officer who will coordinate a response.

- 9.2 If you would like to make a SAR in relation to your own personal data you should make this in writing to the Data Protection Team **BSP International Foundations Ltd, Claydon Business Park, Gipping Road, Great Blakenham, Ipswich, Suffolk IP6 0NL**. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

- 9.3 There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

10. **YOUR DATA SUBJECT RIGHTS**

- 10.1 You have the right to information about what personal data we process, how and on what basis as set out in this policy.

- 10.2 You have the right to access your own personal data by way of a subject access request (see above).

- 10.3 You can correct any inaccuracies in your personal data. To do so, you should contact the Data Protection Team, **BSP International Foundations Ltd, Claydon Business Park, Gipping Road, Great Blakenham, Ipswich, Suffolk IP6 0NL**.

- 10.4 You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so, you should contact the Data Protection Team, **BSP International Foundations Ltd, Claydon Business Park, Gipping Road, Great Blakenham, Ipswich, Suffolk IP6 0NL**.

- 10.5 While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so, you should contact the Data Protection Team, **BSP International Foundations Ltd, Claydon Business Park, Gipping Road, Great Blakenham, Ipswich, Suffolk IP6 0NL.**
- 10.6 You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.
- 10.7 You have the right to object if we process your personal data for the purposes of direct marketing.
- 10.8 You have the right to be notified of a data security breach concerning your personal data.
- 10.9 In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the Data Protection Team, **BSP International Foundations Ltd, Claydon Business Park, Gipping Road, Great Blakenham, Ipswich, Suffolk IP6 0NL.**
- 10.10 You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.