**Data Processing Agreement**

**Last modified:** 23 March 2022

This Data Processing Agreement, including its exhibits, (the “**Agreement**”) governs the Processing of Personal Data by Plutio LTD having a registered business address at 4th Floor Silverstream House, Fitzroy Street, London, W1T 6EB, the United Kingdom (“**Plutio**"). Plutio owns and operates the business management software available at https://www.plutio.com, the related domain names, software, and services (collectively, the ““**Services**). This Agreement governs the Processing of Personal Data submitted by an individual user or an entity through the Services (the “**Client**”). Plutio and the Client are hereby collectively referred to as the “**Parties**” and each individually a “**Party**”.

The Agreement sets out rights and obligations of the Parties regarding the Processing of Personal Data, where Plutio acts in the capacity of the Data Processor and the Client acts in the capacity of the Data Controller. The Agreement is drafted in accordance with Standard Contractual Clauses attached as Appendix I of the Agreement.

By concluding the Agreement, the Client enters into this Agreement on behalf of itself and, to the extent required under applicable Data Protection Law, in the name and on behalf of its authorised affiliates, if and to the extent Plutio processes the Personal Data for which such authorised affiliates qualify as the Data Controller.

|  |
| --- |
| **How to execute this Agreement**   1. This Agreement consists of the main body and Appendix I. 2. This Agreement and its Appendix I have been pre-signed by Plutio. 3. To complete the Agreement, the Client must:    1. Complete the information in the signature box on page 5;    2. Complete the information requested in Exhibit I (highlighted in green);    3. Sign the Agreement; and    4. Send the Agreement to joe@plutio.com specifying, if applicable, the Client number.   Upon receipt of the validly completed Agreement by Plutio to the email address indicated above, this Agreement will become legally binding. |

1. **Definitions**
   1. In this Agreement, the following definitions shall apply:

“**Client’s Data**“ shall mean the Personal Data processed through the Services of which the Client is the Data Controller.

**“Contract”** shall mean a service agreement concluded between the Parties governing the Services.

“**Data Controller**” shall mean a natural or legal person, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

“**Data Protection Law”** means the statutory data privacy and protection regulations applicable to the Client and the Processor protecting the fundamental rights and freedoms of persons with regard to data privacy and the Processing of the Client’s Data by the Processor.

“**Data Subject**” shall mean an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

“**EU**” shall mean European Union.

“**GDPR**” shall mean the Regulation (EU) 2016/679 (General Data Protection Regulation).

**“UK GDPR”** shall mean the UK data protection laws, including, without limitation, the UK Data Protection Act 2018.

“**Instruction**” shall mean an instruction issued by the Client to Plutio and directing Plutio to perform a specific action with regard to the Processing of the Client’s Data in order to achieve compliance with the Data Protection Law.

“**Personal Data**” shall mean any information relating to an identified or identifiable natural person.

“**Data Processor”** shall mean a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller;

“**Processing**” shall mean any operation which is performed on Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“**Sub-processor**” shall mean an entity that Processes Personal Data as a subcontractor of the Data Processor.

1. **Subject matter of Processing** 
   1. The Client has engaged Plutio to provide services to the Client by means of the Contract, and the Parties agree that Plutio shall carry the Processing of the Client’s Data, the categories of which are described in section 4 of this Agreement, pursuant to the terms stated herein.
   2. This Agreement applies to all activities within the scope of the Services and the Contract in the context of which Plutio or any Sub-processor may come into contact with the Client’s Data.
   3. To ensure the transparency of the Processing, the Parties shall keep records of all Processing activities regarding Personal Data, as required by Art. 30 of the GDPR and the UK GDPR.
2. **Scope, nature, and purpose of Processing**
   1. Plutio shall Process the Client’s Data on behalf of the Client as Client’s Data Processor. The scope, extent, and nature of the Processing are the sole purpose of facilitation of the provision of Services by Plutio to the Client.
   2. Plutio shall ensure that any of its officers, directors, employees, consultants, representatives and other natural persons that participate in the Processing of the Client’s Data agree to the same restrictions and conditions as those listed in this Agreement.
   3. The Client as the Data Controller shall be responsible for complying with the applicable Data Protection Law, including, but not limited to, the lawfulness of the Processing and the lawfulness of the transmission (if any) of the Client’s Data to Plutio.
   4. Plutio shall Process the Client’s Data only to the extent required and with the purpose of fulfilling the Plutio’s obligations under the Contract, to the extent necessary for the provision of the Services, and in accordance with the Instructions.
   5. Should Plutio wish to use the Client’s Data for the purposes that are not specified in this section 3, Plutio shall request the Client to provide prior consent in writing.
3. **Categories of Personal Data**
   1. Plutio shall Process all Client’s Data submitted by the Client through the Services. To the extent the Client’s Data contains Personal Data, it may consist of Data Subjects’ names, surnames, contact details, payment and commercial information.
   2. No special categories of Personal Data as defined in Art. 9(1) of the GDPR are processed according to this Agreement.
4. **Categories of Data Subjects**
   1. The affected Data Subjects shall include natural persons, Client’s clients, business partners, prospects, and staff members, whose personal data is supplied by the Client to Plutio through the Services.
   2. Plutio shall not interact with the Data Subjects directly in any manner without Client’s prior approval.
5. **Duration of Processing**
   1. Except where this Agreement expressly stipulates any surviving obligation, this Agreement shall follow the term of the Contract.
   2. Plutio shall Process the Client’s Data for as long as the Client’s Data is necessary for the purpose described in section 3 of this Agreement.
   3. Plutio shall return to the Client or securely erase Client’s Data from its storage systems as soon as the Client’s Data is no longer necessary for the purpose described in section 3 of this Agreement or the Client requests Plutio to do so. Upon request of the Client, Plutio shall provide the Client with a proof of erasure of the Client’s Data.
6. **Security of Processing**
   1. Plutio shall exercise a reasonable degree of care to protect the Client’s Data from misuse, unauthorised access, disclosure, and transfer to any third parties unauthorised by the Client. Such measures shall include, without limitation:
      1. Maintaining adequate access control mechanisms (e.g., two-factor authentication, password protection, and limited access) covering any systems, servers, or files in which the Client’s Data is stored;
      2. Encryption;
      3. DDOS mitigation;
      4. Limiting access to the Client’s Data by Plutio’s officers, directors, employees, consultants, and representatives only to the purpose stated in section 3 of this Agreement; and
      5. Conducting regular information security audits.
   2. Plutio hereby declares that it has taken appropriate technical and organisational measures in accordance with Art. 32 GDPR and the UK GDPR to keep the Client’s Data secure and protected against unauthorised or unlawful processing and accidental loss, destruction or damage, and undertakes to continue doing so during the term of this Agreement.
   3. If, under applicable laws, Plutio is compelled to disclose the Client’s Data, Plutio shall inform the Client before any such mandatory disclosure within 24 hours after such a disclosure is requested.
   4. Any significant changes to the security measures listed in section 7.1 of the Agreement shall be documented by Plutio and reported to the Client.
   5. Plutio shall appropriately document the technical and organisational measures actually implemented (including each update) for the Processing of the Client’s Data and will hand out the then current version of such documentation to the Client, upon Client’s request (e.g., for audit purposes).
   6. For the purpose of documentation, Plutio shall be entitled to provide evidence for the implementation of the security measures by providing up-to-date attestations, reports or extracts from independent bodies that scrutinise and confirm the Processing of the Client’s Data is in accordance with the agreed to measures herein.
7. **Correction and deletion of Personal Data** 
   1. Plutio may be required to correct, erase and/or block the Client’s Data if and to the extent the functionality of the Services does not allow the Client to do so. However, Plutio shall not correct, erase or block the Client’s Data, unless instructed by the Client.
   2. Unless the Data Protection Law provides otherwise, there shall not be any direct communication between the Data Subjects and Plutio. In the event that a Data Subject does apply directly to Plutio in writing with a request to exercise Data Subject’s legitimate rights, e.g., to request the correction or deletion of his/her Personal Data, Plutio shall forward this request to the Client without undue delay and shall not respond directly to the Data Subject.
8. **Data Processor’s obligations**
   1. In addition to any other obligations set out in this Agreement, Plutio shall:
      1. Comply with all laws and regulations applicable to the Plutio’s business activities;
      2. Ensure that persons authorised to Process the Client’s Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Plutio shall regularly train those persons to whom it grants access to the Client’s Data on IT security and privacy law compliance. The undertaking to data secrecy shall continue after the termination of this Agreement;
      3. Ensure that any natural person acting under the authority of Plutio who has access to the Personal Data does not process them except on instructions from the Client;
      4. Assist the Client in compliance with Client’s obligations under the applicable Data Protection Law;
      5. Make available to the Client all information necessary to demonstrate compliance with Plutio ’s obligations under the Agreement, the Data Protection Law, and allow for and contribute to audits, including inspections, conducted by the Client or another auditor mandated by the Client;
      6. Appoint a data protection officer if it is legally obliged to do so or, if it is not obliged to do so, a contact person for data protection issues;
      7. Provide the Client, upon request in writing, with the name and contact details of its data protection officer or the contact person for data protection issues;
      8. Monitor the Processing by way of regular reviews concerning the performance of and compliance with this Agreement, the Contract, and the applicable Data Protection Law;
      9. At Client’s written request, reasonably support the Client in dealing with requests from individual Data Subjects and/or a supervisory authority with respect to the Processing of the Personal Data hereunder;
      10. Assist the Client with the implementation of appropriate technical and organisational measures in order to respond to applications by the Data Subjects for the exercise of their rights (in particular, Art. 13 to 23 of the GDPR);
      11. Provide at minimum the information in accordance with Art. 33(3) of the GDPR in the case of a Personal Data breach;
      12. Communicate the necessary information to the Data Subjects after a Personal Data breach pursuant to Art. 34 of the GDPR and the UK GDPR; and
      13. If applicable under Art. 35 of the GDPR and the UK GDPR, conduct prior (i.e. before the start of the processing) data protection impact assessments and, if necessary, consult with a supervisory authority.
   2. Plutio commits to observe any and all other duties that are imposed to Plutio by the Data Protection Law (if applicable, Art. 28 of the GDPR).
   3. Plutio shall collaborate with Client’s data protection officer to generate the records of processing activities, (if applicable, pursuant to Art. 30 of the GDPR), and provide all the necessary details to the Client.
9. **Sub-processors** 
   1. The Client hereby authorises Plutio to engage Sub-processors as specified in Annex III to the Agreement, provided that Plutio remains responsible for any acts or omissions of its Sub-processors in the same manner as for its own acts and omissions hereunder.
   2. Plutio may remove or appoint suitable and reliable other Sub-processor(s) at its own discretion in accordance with the following conditions:
      1. Plutio shall inform the Client fourteen (14) days in advance of any envisaged changes to the list of Sub-processors;
      2. If the Client has a legitimate data protection related reason to object to Plutio’s use of Sub-processor(s), the Client shall notify Plutio within fourteen (14) days after receipt of the Plutio’s notice;
      3. If the Client does not object during this time period, the new Sub-processor(s) shall be deemed accepted;
      4. If the Client objects to the use of the Sub-processor(s) concerned, Plutio shall have the right to cure the objection through one of the following options (to be selected at Plutio’s sole discretion):
         1. Plutio will abort its plans to use the Sub-processor(s) with regard to the Client’s Data; or
         2. Plutio will take corrective steps and proceed to use the Sub-processor(s) with regard to the Client’s Data.
      5. If Plutio decides not to implement option 10.2.d.i or 10.2.d.ii above, Plutio shall notify the Client without undue delay. In this case, the Client shall be entitled within further fourteen (14) days to notify in writing Plutio about its termination of the Agreement and any such termination would become effective upon the expiry of the second (2nd) calendar month after Processor’s receipt of the termination notice.
   3. Plutio shall pass on to its subcontractors acting as the Sub-processors Plutio’s obligations under this Agreement.
   4. Plutio shall ensure that, where the Client’s Data is transferred from the territory where the Client is located, appropriate safeguards, including the transfer mechanisms listed in section 14, are applied by Plutio to ensure that the Client’s Data is further processed in a secure manner compliant with this Agreement and the Data Protection Law.
10. **Personal Data breaches**
    1. Within 24 hours after Plutio becomes aware of any unauthorised use or disclosure of the Client’s Data, Plutio shall promptly report the unauthorised use or disclosure of the Client’s Data to the Client.
    2. Plutio shall cooperate with any remediation that the Client, in its discretion, determines is necessary to (i) address any applicable reporting requirements and (ii) mitigate any effects of unauthorised use or disclosure of the Client’s Data.
    3. In consultation with the Client, Plutio must take appropriate measures to secure the Client’s Data and limit any possible detrimental effect on the Data Subjects. Where obligations are placed on the Client under the Data Protection Law, Plutio shall provide commercially reasonable assistance in meeting them.
11. **Notifications** 
    1. If Plutio receives a request, subpoena or court order (including through an obligation due to legal provisions or official injunctions from state authorities) requesting to provide any Client’s Data to an authority, Plutio shall attempt to redirect the relevant authority to request that data directly from the Data Controller, and notify the Client without undue delay.
    2. Where the Client’s Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while in Plutio’s control, Plutio shall notify the Client of such action without undue delay.
12. **Instructions** 
    1. The Instructions to Plutio are initially laid out in this Agreement. However, the Client shall be entitled to issuing modifications to Instructions and to issue new Instructions, subject to feasibility.
    2. The Client shall designate a person competent to issue the Instructions. Modifications or new Instructions shall be issued in writing and shall need to be agreed between the Parties as a contract modification/change request under this Agreement.
    3. Plutio shall not be obligated to perform a comprehensive legal examination and shall in no event render any legal services to the Client.
    4. Plutio shall not be responsible for any consequences of the Instructions issued by the Client and the Client shall indemnify and hold Plutio harmless against any damages and third-party claims resulting from the Instruction.
    5. Unless otherwise agreed, Plutio shall be entitled to charge any efforts incurred in connection with the Instructions on time and material basis.
13. **Transfer mechanisms**
    1. Plutio makes available the transfer mechanisms, namely, concluding data processing agreements based on the Standard Contractual Clauses, which shall apply to any transfers of the Personal Data under this Agreement from the EU, the European Economic Area and/or their member states, Switzerland, and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of the GDPR.
    2. For any other cross-body transfers of Personal Data, Plutio shall take steps necessary to ensure the compliance with the applicable data protection rules and regulations.
14. **Miscellaneous** 
    1. No modification of this Agreement shall be valid and binding unless made in writing and then only if such modification expressly states that such modification applies to the regulations of this Agreement. The foregoing shall also apply to any waiver or modification of this mandatory written form.
    2. This Agreement shall take precedence over any conflicting provisions of the Contract.
    3. This Agreement will commence on the date when both Parties sign the Agreement and continue until terminated earlier by either Party.
    4. Either Party may terminate this Agreement for any reason upon thirty (30) calendar days’ notice to the other Party.
    5. Each Party may terminate this Agreement with immediate effect by delivering a notice of the termination to the other Party if:
       1. The other Party fails to perform, has made or makes any inaccuracy in, or otherwise materially breaches, any of its obligations, covenants, or representations; and
       2. The failure, inaccuracy, or breach continues for a period of thirty (30) calendar days’ after the injured Party delivers notice to the breaching Party reasonably detailing the breach.
    6. If either Party becomes insolvent, bankrupt, or enters receivership, dissolution, or liquidation, the other Party may terminate this Agreement with immediate effect.
    7. Upon expiration or termination of this Agreement or on Client’s request, Plutio shall:
       1. Promptly securely delete or return any Client’s Data available to Plutio and any other information and documents, provided by the Client; and
       2. Deliver to the Client a certificate confirming Plutio’s compliance with the destruction obligation under this section 15.7.
    8. Neither Party may assign this Agreement or any of their rights or obligations under this Agreement without the other Party’s prior consent.
    9. The Parties shall attempt to resolve any dispute arising out of or relating to this Agreement in a good faith through negotiations between senior executives of the Parties, who have authority to settle the same. If the matter is not resolved by negotiation within thirty (30) days of receipt of a written invitation to negotiate, the dispute shall be resolved by using binding arbitration services.
    10. The headings used in this Agreement and its division into sections, schedules, exhibits, appendices, and other subdivisions do not affect its interpretation.
    11. If there is any inconsistency between the terms of this Agreement and those in any document entered into under this Agreement, the terms of this Agreement shall prevail. The Parties shall take all necessary steps to conform the inconsistent terms to the terms of this Agreement.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Plutio - Data Processor** |  |  | **The Client - Data Controller** |
| Name: | Leo Bassam |  | Name: |  |
| Title: | CEO |  | Title: |  |
| Date: | April 25, 2022 |  | Date: |  |
| Signature: | page2image22766976 |  | Signature: |  |

**Attached Exhibit I:** UK Standard Contractual Clauses for controllers to pr

ocessors

**EXHIBIT I**

**The standard contractual clauses for international transfers from controllers to processors**

|  |  |
| --- | --- |
| **Parties** |  |
| Name of the data exporting organisation: | Click here to enter text. |
| Address | Click here to enter text. |
| Telephone | Click here to enter text. |
| Fax | Click here to enter text. |
| Email | legal@plutio.com |
| Other information needed to identify the organisation | Click here to enter text. |
|  | (the data **exporter**”) |
|  | And |
| Name of the data importing organisation: | Plutio LTD |
| Address | 4th Floor Silverstream House, Fitzroy Street, London, W1T 6EB  Country: United Kingdom |
| Email | [joe@plutio.com](mailto:joe@plutio.com) |
| Other information needed to identify the organisation | Trade License Number: 09856706 |
|  | (the data **importer**”) |
| Clause 1. Definitions | For the purposes of the Clauses: (a)‘personal data’, ‘special categories of data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data subject’ and ‘Commissioner’ shall have the same meaning as in the UK GDPR; |
|  | (b) ‘the data exporter’ means the controller who transfers the personal data; |
|  | (c) ‘the data importer’ means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country’s system covered by UK adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018; |
|  | (d) ‘the sub-processor’ means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract; |
|  | (e) ‘the applicable data protection law’ means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the UK; |
|  | (f) ‘technical and organisational security measures’ means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. |
| Clause 2. Details of the transfer | The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses. |
| Clause 3. Third-party beneficiary clause |  |
| 3(1) | The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary. |
| 3(2) | The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. |
| 3(3) | The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses. |
| 3(4) | The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law. |
| Clause 4. Obligations of the data exporter | The data exporter agrees and warrants: |
| 4(a) | that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the Commissioner) and does not violate the applicable data protection law; |
| 4(b) | that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter’s behalf and in accordance with the applicable data protection law and the Clauses; |
| 4(c) | that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract; |
| 4(d) | that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation; |
| 4(e) | that it will ensure compliance with the security measures; |
| 4(f) | that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not covered by adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 Data Protection Act 2018; |
| 4(g) | to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the Commissioner if the data exporter decides to continue the transfer or to lift the suspension; |
| 4(h) | to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information; |
| 4(i) | that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; |
| 4(j) | that it will ensure compliance with Clause 4(a) to (i). |
| Clause 5. Obligations of the data importer | The data importer agrees and warrants: |
| 5(a) | to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract; |
| 5(b) | that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract; |
| 5(c) | that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred; |
| 5(d) | that it will promptly notify the data exporter about:(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;(ii) any accidental or unauthorised access; and(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so; |
| 5(e) | to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the Commissioner with regard to the processing of the data transferred; |
| 5(f) | at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the Commissioner; |
| 5(g) | to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter; |
| 5(h) | that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent; |
| 5(i) | that the processing services by the sub-processor will be carried out in accordance with Clause 11; |
| 5(j) | to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter. |
| Clause 6. Liability |  |
| 6(1) | The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered. |
| 6(2) | If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities. |
| 6(3) | If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses. |
| Clause 7. Mediation and jurisdiction |  |
| 7(1) | The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject: (a) to refer the dispute to mediation, by an independent person or, where applicable, by the Commissioner;  (b) to refer the dispute to the UK courts. |
| 7(2) | The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law. |
| Clause 8. Cooperation with supervisory authorities | The data exporter agrees to deposit a copy of this contract with the Commissioner if it so requests or if such deposit is required under the applicable data protection law. |
| 8(2) | The parties agree that the Commissioner has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law. |
| 8(3) | The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b). |
| Clause 9. Governing law | The Clauses shall be governed by the law of the United Kingdom, England and Wales. |
| Clause 10. Variation of the contract | The parties undertake not to vary or modify the Clauses. This does not preclude the parties from (i) making changes permitted by Paragraph 7(3) & (4) of Schedule 21 Data Protection Act 2018; or (ii) adding clauses on business related issues where required as long as they do not contradict the Clause. |
| Clause 11. Sub-processing |  |
| 11(1) | The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor’s obligations under such agreement. |
| 11(2) | The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses. |
| 11(3) | The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the laws of the country of the UK where the exporter is established. |
| 11(4) | The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the Commissioner. |
| Clause 12. Obligation after termination |  |
| 12(1) | The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore. |
| 12(2) | The data importer and the sub-processor warrant that upon request of the data exporter and/or of the Commissioner, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1. |
| Additional commercial clauses | The parties are able to add additional commercial clauses.When including additional commercial clauses, the parties should ensure that these clauses do not in any way:overlap with or contradict the standard contractual clauses;reduce the level of protection which the data importer is required to provide for the personal data; orreduce the rights of data subjects, or make it any more difficult for them to exercise their rights. |
| Indemnification | LiabilityThe parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.Indemnification is contingent upon: (a) the data exporter promptly notifying the data importer of a claim; and  (b) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim. |
| Priority of standard contractual clauses | The Standard Contractual Clauses take priority over any other agreement between the parties, whether entered into before or after the date these Clauses are entered into.Unless the Clauses are expressly referred to and expressly amended, the parties do not intend that any other agreement entered into by the parties, before or after the date the Clauses are entered into, will amend the terms or the effects of the Clauses, or limit any liability under the Clauses, and no term of any such other agreement should be read or interpreted as having that effect. |
| On behalf of the data exporter:Name (written out in full):Click here to enter text.Position:Click here to enter text.Address:Click here to enter text.Other information necessary in order for the contract to be binding (if any):Signature:Click here to enter text. | |
| On behalf of the data importer:Name (written out in full):Leo BassamPosition:CEOAddress:4th Floor Silverstream House, Fitzroy Street, London, W1T 6EB, United KingdomOther information necessary in order for the contract to be binding (if any):Trade License Number: 09856706Signature: page2image22766976 | |
| Date of the Standard Contractual Clauses: Click here to enter text. | |

|  |  |
| --- | --- |
| Appendix 1 |  |
| This Appendix forms part of the Clauses and must be completed and signed by the parties. | |
| Data exporter | |
| The data exporter is (please specify briefly your activities relevant to the transfer): the user of the business management platform https://www.plutio.com.The data exporter is using the personal data which is being transferred for the following purposes or activities: The data exporter is using the personal data which is being transferred for the following purposes or activities:  ☐ Staff administration, including permanent and temporary staff, including appointment or removals, pay, discipline; superannuation, work management, and other personnel matters in relation to the data exporter’s staff.  ☐ Advertising, marketing and public relations of the data exporter’s own business or activity, goods or services.  ☐ Accounts and records, including   * + keeping accounts relating to the data exporter’s business or activity;   + deciding whether to accept any person or organisation as a customer;   + keeping records of purchases, sales or other transactions, including payments, deliveries or services provided by the data exporter or to the data exporter;   + keeping customer records   + records for making ﬁnancial or management forecasts; and   + other general record keeping and information management. | |
| Data importer | |
| The data importer is the owner and operator of the business management platform https://www.plutio.com.The data importer’s activities for the data exporter, which are relevant to the transfer are:☐ Accounts and records services, includingkeeping accounts;deciding whether to accept any person or organisation as a customerkeeping records of purchases, sales or other transactions, including payments, deliveries or services provided by the data exporter or to the data exporter;records for making ﬁnancial or management forecastsother general records and information management services.☐ Administration services relating to membership or supporter records.☐ Advertising, marketing, and public relations services.☐ Information and databank administration, including the maintenance of information or databanks as a reference tool or general resource. This includes catalogues, lists, directories and bibliographic databases.☐ IT, digital, technology or telecom services, including provision of technology products or services, telecoms and network services, digital services, hosting, cloud and support services or software licensing☐ Staff administration services, including appointment or removals, pay, discipline; superannuation, training, employee benefits, work management, and other personnel matters in relation to the data exporter’s staff. | |
| Data subjects | |
| The personal data transferred concern the following categories of data subjects (please specify): ☐ customers and clients (including their staff)  ☐ suppliers (including their staff)  Each category includes current, past and prospective data subjects. Where any of the following is itself a business or organisation, it includes their staff. | |
| Categories of data | |
| The personal data transferred concern the following categories of data (please specify): The following is a list of standard descriptions of categories of data:  ☐ Personal details, including any information that identiﬁes the data subject and their personal characteristics, including: name, address, contact details, age, date of birth, sex, and physical description.  ☐ Goods or services provided and related information, including details of the goods or services supplied, licences issued, and contracts. | |
| Special categories of data (if appropriate) | |
| The personal data transferred concern the following special categories of data (please specify): none | |
| Processing operations | |
| The personal data transferred will be subject to the following basic processing activities (please specify):☐ Receiving data, including collection, accessing, retrieval, recording, and data entry☐ Holding data, including storage, organisation and structuring☐ Using data, including analysing, consultation, testing, automated decision making and profiling☐ Updating data, including correcting, adaptation, alteration, alignment and combination☐ Protecting data, including restricting, encrypting, and security testing☐ Sharing data, including disclosure, dissemination, allowing access or otherwise making available☐ Returning data to the data exporter or data subject☐ Erasing data, including destruction and deletion | |

| Appendix 2 |  |
| --- | --- |
| This Appendix forms part of the Clauses and must be completed and signed by the parties.The following is the description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c): the use of firewalls and safe server rooms; secured networks; limited access to personal data by the data importer’s staff; anonymisation of personal data; proper access control systems; the controlled provision of user rights and supervision of their use; providing instructions for data processors; the thorough selection of competent subcontractors who comply with industry standards for information security management; and data processing agreements concluded with subcontractors. | |
| DATA EXPORTERName: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Authorised Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| DATA IMPORTERName: Leo Bassam Authorised Signature:  page2image22766976 | |