DATAFLOW
Financial Software Solutions

General Data Protection Regulation

The General Data Protection Regulation (“GDPR”) came into effect in May 2018 and applies to all businesses who hold or otherwise process personal data.

Dataflow (UK) Ltd understands that its products and services may form part of the controls and processes that businesses will implement in order to meet some of their own GDPR obligations. Although we do not hold any personal data on behalf of client, there is no substitute for customers seeking their own legal advice if they are unsure about the implications of the GDPR on their businesses.

Dataflow (UK) Ltd has introduced a comprehensive GDPR training program, aimed at all employees, to ensure they understand the basics of data protection law and to educate them to recognise, respond and to report privacy breaches.

Dataflow (UK) Ltd’s internal policy requires all new products and processes affecting personal data to undertake a Privacy Impact Valuation ("PIV") prior to launch in order to anticipate and minimise privacy risks and prevent intrusive behaviour.

Dataflow (UK) Ltd has established an incident reporting policy for internal escalation (as required) of incidents, including those which may involve personal data.

Dataflow (UK) Ltd has also established training and procedures on how to recognise and respond to data subject access requests, with the importance of identity checks and detailing how to respond to requests for data portability and the rectification and erasure of personal data.

DEFINITIONS AND INTERPRETATION

A. Definitions

"Affiliate" means:

(i) any subsidiary, subsidiary undertaking or holding company of the Customer and any subsidiary or subsidiary undertaking of any such holding company for the time being; and/or

(ii) any company controlling (directly or indirectly) or under common control with the Customer ('control' for the purposes of this definition meaning direct or indirect beneficial ownership of 50% or more of the share capital, stock or other participating interest carrying the right to vote or to distribution of profits of that entity or person, as the case may be);

"Applicable Laws" are the laws of England;

"Appropriate Safeguards" means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under DP Laws from time to time;

"Business Day" means a day other than a Saturday, Sunday or public holiday in England when banks in London are open for business;

"Complaint" means a complaint or request relating to either party's obligations under Data Protection Laws relevant to this Addendum, including any compensation claim from a Data Subject or any notice, investigation or other action from a Supervisory Authority;

"Controller to Processor SCCs" means the Standard Contractual Clauses (processors) for the purposes of Article 26(2) of Directive 95/46/EC set out in Decision 2010/87/EC as the same are revised or updated from time to time by the European Commission;

"Data Subject Request" means a request made by a Data Subject to exercise any rights of Data Subjects under DP Laws;

"DPIA" means a data protection impact assessment, in accordance with DP Laws;

"DP Laws" means any law, enactment, regulation, regulatory policy, ordinance or subordinate legislation relating to the processing, privacy, and use of Personal Data, as applicable to the Customer, Dataflow and/or the Services, including:

(a) in the UK:

(i) the Data Protection Act 1998 ("**DPA 1998**"), the Data Protection Act 2018 (when enacted and applicable) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any laws or regulations implementing Council Directives 95/46/EC ("**Data Protection Directive**") or 2002/58/EC ("**ePrivacy Directive**"); and/or

(ii) the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("**GDPR**") together with any law implementing GDPR in the UK; and/or

(iii) any national laws or regulations created as a result of the United Kingdom's vote to leave the European Union ("**Revised UK DP Law**"); and

(b) in EU countries: the Data Protection Directive or the GDPR (once applicable); the ePrivacy Directive, the EU Regulation repealing the ePrivacy Directive (once applicable) and all relevant EU or EEA member state ("**Member State**") laws or regulations giving effect to or corresponding with any of them; and

(c) any judicial or administrative interpretation of any of the above, and any guidance, guidelines, codes of practice, approved codes of conduct or approved certification mechanisms issued by any relevant Supervisory Authority,

in each case, as in force and applicable, and as may be amended, supplemented or replaced from time to time;

"DP Losses" means all liabilities and amounts, including all:

(a) costs (including legal costs), claims, demands, actions, settlements, charges, procedures, expenses, losses and damages (including relating to material or non-material damage); and

(b) to the extent permitted by Applicable Law:

(i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority; and/or

(ii) compensation to a Data Subject ordered by a Supervisory Authority;

"Good Industry Practice" means at any time the exercise of that degree of care, skill, diligence, prudence, efficiency, foresight and timeliness which would be reasonably expected at such time from a leading and competent professional supplier of services similar to the Services provided under this Addendum, such supplier seeking to comply with its contractual obligations in full and complying with all applicable laws in respect of such services, using personnel who are suitably skilled and experienced to perform tasks assigned to them and in sufficient number to ensure that supplier's obligations are fulfilled;

"Personal Data Breach" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Protected Data;

"Personnel" means employees, workers, sub-contractors, suppliers, apprentices, authorised third parties;

"Protected Data" means Personal Data received from or on behalf of the Customer, or otherwise obtained in connection with the performance of Dataflow's obligations under this Addendum;

"Services" means the services provided by the supplier to the Customer as described in the Agreement;

"Sub-Processor" means another Data Processor engaged by Dataflow for carrying out processing activities in respect of the Protected Data on behalf of the Customer which relate directly to the provision of the Services. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services, nor measures to ensure the confidentiality, availability, integrity, and resilience of the hardware and software of processing equipment;

"Supervisory Authority" means any independent public authority which is established by a Member State pursuant to DP Laws.

B. Interpretation

I. "**Data Controller**" (or controller) and "**Data Processor**" (or processor) have the meanings given to those terms (or to the terms 'controller' (for Data Controller) or 'processor' (for Data Processor)) in DP Laws.

II. "**Data Subject**", "**Personal Data**" and "**processing**" referred to in this schedule and in the Addendum shall have the meanings given to those terms in DP Laws (and related terms such as "**process**" have corresponding meanings).

III. References in this Addendum to the DPA 1998 or the Data Protection Directive and to terms defined in that Act or in that Directive shall be replaced with or incorporate (as the case may be) references to any laws replacing, amending, extending, re-enacting or consolidating such Act or Directive (including particularly the GDPR and/or the Revised UK DP Law) and the equivalent terms defined in such laws, once in force and applicable.

IV. To the extent that a term of this Addendum requires the performance by a party of an obligation "in accordance with DP Laws" (or similar), unless otherwise expressly agreed in this Addendum, this requires performance in accordance with the relevant requirements of such DP Laws as are in force and applicable at the time of performance (if any).

V. Any reference to the consent of the Customer shall be construed as a reference to any such consent being granted at the absolute discretion of the Customer unless the relevant provision expressly provides to the contrary.

VI. Any obligation of Dataflow to do something includes an obligation to procure that it is done and any obligation of Dataflow not to do something includes an obligation not to allow that thing to be done.

VII. Any words following the terms "including", "include", "in particular", "for example" or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms.

VIII. References to time are to the time in London, England.

IX. References to any statute, or to any statutory provision, including any regulation, statutory instrument, or other subordinate legislation derived from such statutory sources, shall include references to any statute or other statutory provision which amends, extends, consolidates or replaces the original statutory reference or which subsequently affects any such revised statutory reference.

X. Customer also includes Customer's Affiliates.

1. DATA PROTECTION

1.1 **Processor/Controller**

1.1.1 The Parties agree that, for the Protected Data, the Customer shall be the Data Controller and Dataflow shall be the Data Processor.

1.2 **Compliance with DP Laws and obligations**

1.2.1 Each party shall comply with DP Laws and with their respective obligations under this Addendum in connection with the processing of Protected Data and the provision of the Services under this Addendum.

1.2.2 Dataflow shall procure that any Sub-Processor that has access to Protected Data shall comply with obligations materially similar to Dataflow's obligations under this Addendum.

1.2.3 The Customer and Dataflow shall obtain and maintain all relevant regulatory registrations and notifications as are required under DP Laws.

1.3 **Details of processing and instructions**

1.3.1 The processing to be carried out by Dataflow under this Addendum shall comprise the processing set out in Appendix 1 (*Supplier GDPR Questionnaire*), as updated from time to time by the Customer or Dataflow. Dataflow undertakes that when such updates occur, the standards of data processing will be of an equivalent or higher standard than those in this Addendum, will be in accordance with Good Industry Practice and shall comply with DP Laws.

1.3.2 Insofar as Dataflow processes Protected Data on behalf of the Customer, Dataflow:

(a) unless required to do otherwise by Applicable Law, shall (and shall ensure each Sub Processor and each natural person acting under its authority shall) process the Protected Data only on and in accordance with the Customer's documented instructions in the Agreement and as set out in this Clause 1.3 and Appendix 1 *(Supplier GDPR Questionnaire)*, and as updated by the Parties from time to time ("**Processing Instructions**") provided that if such Processing Instructions require Dataflow to implement any measures or processes over and above those in place at the time of receiving the Processing Instructions, Dataflow shall not be required to implement such measures and processes until such time as the Parties have agreed in writing on who bears the cost for implementing such measures and processes; and

(b) if Applicable Law requires it to process Protected Data other than in accordance with the Processing Instructions, shall notify the Customer of any such requirement before processing the Protected Data (unless that law prohibits such information on important grounds of public interest); and

(c) to the extent required by DP Laws, shall promptly inform the Customer in writing if, in Dataflow's reasonable opinion, a Processing Instruction infringes DP Laws and explain the reasons for its opinion, provided that this shall be without prejudice to Clause 1.2.1; and

(d) shall comply with all DP Laws applicable to the manner of its provision of any Services and shall inform the Customer as soon as reasonably practicable on becoming aware of any change to DP Laws which might reasonably be expected to have an impact upon the provision of the Services.

1.4 **Technical and organisational measures**

1.4.1 Dataflow shall implement and maintain, at its cost and expense, technical and organisational measures in accordance with Good Industry Practice in relation to the processing of Protected Data by Dataflow as a Data Processor:

(a) such that their processing will meet the requirements of DP Laws and ensure the protection of the rights of Data Subjects; and

(b) so as to ensure a level of security in respect of Protected Data processed by it appropriate to the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed; and

(c) without prejudice to Clause 1.9, insofar as is possible and in accordance with DP Laws, to assist the Customer in the fulfilment of the Customer's obligation to respond to Data Subject Requests relating to Protected Data provided that the Customer shall be responsible for Dataflow's reasonable costs and expenses arising from such co-operation and assistance.

1.5 **Security of processing**

1.5.1 Without prejudice to Clause 1.4.1(b), Dataflow shall, in respect of the Protected Data processed by it under this Addendum comply with the requirements regarding security of processing set out in DP Laws (as applicable to Data Processors) and in this Addendum.

1.6 **Using other processors**

1.6.1 If Dataflow engages a Sub-Processor for carrying out any processing activities in respect of the Protected Data on behalf of the Customer, Dataflow shall (prior to any processing of the Protected Data by the Sub-Processor) appoint the Sub-Processor under a binding written contract, with enforceable data protection obligations on materially equivalent terms as apply to Dataflow under this Addendum ("**Processor Contract**"). In particular, in the Processor Contract, the Sub-Processor shall:

(a) provide sufficient guarantees to implement appropriate technical and organisational measures so as to ensure a level of security in respect of Protected Data processed by it appropriate to the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed; and

(b) oblige any Sub-Processors to procure that their Sub-Processors must comply with conditions materially equivalent to this Clause 1.6.

1.6.2 Dataflow shall promptly upon request by the Customer provide the relevant details of any such Processor Contract to the Customer.

1.6.3 Dataflow shall, where that Sub-Processor fails to fulfil its data protection obligations in accordance with the Processor Contract, remain fully liable to the Customer for the performance of that Sub-Processor's obligations.

1.7 Dataflow shall immediately cease using a Sub-Processor upon receiving written notice from the Customer requesting that the Sub-Processor ceases processing Protected Data for security reasons or concerns about the Sub-Processor's ability to carry out the relevant processing in compliance with DP Laws or this Addendum.

1.8 **Personnel requirements**

1.8.1 Dataflow shall ensure that the Personnel processing Protected Data have entered into a binding contractual obligation with Dataflow to keep the Protected Data confidential (except where disclosure is required in accordance with Applicable Law, in which case Dataflow shall, where practicable and not prohibited by such Applicable Law, notify the Customer of any such requirement before such disclosure); and

1.8.2 Dataflow shall take all reasonable steps to ensure the reliability of the Personnel processing Protected Data and that the Personnel processing Protected Data receive adequate training on compliance with the relevant parts of this Addendum and the DP Laws applicable to the processing.

1.9 **Data Subject rights**

1.9.1 Dataflow shall promptly record and then refer all Data Subject Requests it receives to the Customer within three working days of receipt of the request.

1.10 **Assistance with the Customer's compliance**

1.10.1 Without prejudice to Clause 1.2.1 and subject to Clause 1.10.2, Dataflow shall provide reasonable assistance (taking into account the nature of processing and the information available to Dataflow) to the Customer in ensuring compliance with the Customer's obligations under DP Laws with respect to:

(a) security of processing; and

(b) any remedial action and notifications to be taken in response to any Personal Data Breach or Complaint, including regarding any notification of the Personal Data Breach to Supervisory Authorities and/or communication to any affected Data Subjects, including in accordance with Clause 1.13.4; and

(c) DPIAs or prior consultation with a Supervisory Authority regarding high risk processing, by providing such information and cooperation as the Customer may reasonably require for the purpose of assisting the Customer in respect of the same.

1.10.2 The Customer shall pay Dataflow's reasonable costs of providing the assistance in Clause 1.10.1.

1.10.3 Unless it is unlawful to do so, Dataflow shall inform Customer in a reasonable time if it makes any notification under 1.10.1(b).

1.11 **International data transfers**

1.11.1 Unless the transfer is based on an "adequacy decision", is otherwise "subject to Appropriate Safeguards" or if a "derogation for specific situations" applies, each within the meanings given to them in DP Laws, Dataflow shall not transfer any Protected Data to any country outside the United Kingdom or the European

Economic Area ("**EEA**") or to any international organisation (an "**International Recipient**") without the Customer's prior written consent. To the extent that any Affiliate or Sub-processor engaged by Dataflow is located in a country outside the EEA which has not been recognised as providing an "adequate level of protection" by the European Commission, Dataflow shall take such steps as are necessary to ensure an adequate level of protection for the Protected Data including by entering into Controller to Processor SCCs with the Affiliate or Sub-processor.

1.11.2 Where transfer of Protected Data to an International Recipient occurs, Dataflow shall ensure that such transfer (and any onward transfer):

(a) is pursuant to a written contract (as referred to in Clauses 1.6.1, 1.8.1 and 1.12.1), including materially equivalent obligations on the Sub-Processor in respect of Protected Data (in particular relating to security and confidentiality) as apply to Dataflow under this Addendum; and

(b) is effected by way of Appropriate Safeguards; and

(c) complies with the relevant parts of Clause 1.3; and

(d) otherwise complies with DP Laws to the extent applicable.

1.12 **Records**

1.12.1 Dataflow shall maintain complete, accurate and up to date written records of all categories of processing activities carried out on behalf of the Customer, containing:

(a) the name and contact details of the Data Processor(s) and Sub Processors and of Dataflow's representative and data protection officer (if any); and

(b) the categories of processing carried out on behalf of each Data Controller; and

(c) where applicable, details of transfers of Protected Data to an International Recipient, including the identification of that International Recipient and the relevant countries to which such data is transferred, and details of the Appropriate Safeguards used; and

(d) a description of the technical and organisational security measures referred to in Clause 1.4.1(b).

1.13 **Compliance, information and audit**

1.13.1 Dataflow shall, and shall procure that its Sub-Processors, make available to the Customer on request in a timely manner:

(a) copies of the records under Clause 1.12; and

(b) such other information as the Customer reasonably requires to demonstrate Dataflow's compliance with its obligations under DP Laws and this Addendum.

1.13.2 Where Customer reasonably believes that Dataflow has committed a breach of this Addendum, or if it is required as part of Customer's obligations to a Supervisory Authority, Dataflow shall allow for and contribute to any audit conducted by the Customer or another auditor mandated by the Customer for the purpose of demonstrating compliance by Dataflow with its obligations under this Addendum, provided that the Customer shall:

(a) give Dataflow reasonable prior written notice of such audit and/or inspection and ensures that any auditor is subject to binding obligations of confidentiality and that such audit or inspection is undertaken (where practicable) during normal business hours; and

(b) where the Customer wishes to conduct more than one audit or inspection every 12 months, pay Dataflow's reasonable costs of allowing or contributing to audits or inspections.

1.13.3 If any audit or inspection reveals a breach by Dataflow of its data protection obligations under this Addendum, Dataflow shall promptly remedy, at its own cost and expense, any breach or potential breach by Dataflow of its obligations under this Addendum. In such circumstances, the Customer reserves the right to require Dataflow to pay the reasonable costs of the Customer or its mandated auditors, of the audit or inspection (or such part of the audit or inspection that relates to the area of non-compliance).

1.13.4 The Customer may share any notification, details, records or information provided by or on behalf of Dataflow under this Clause 1.13 or Clause 1.14 with its professional advisors and/or to the extent required, the Supervisory Authority.

1.14 **Notification of Personal Data Breaches and Complaints**

1.14.1 In respect of any Personal Data Breach involving Dataflow (or a Sub-Processor), Dataflow shall:

(a) notify the Customer of the Personal Data Breach without undue delay (but in no event later than 12 hours after becoming aware of the Personal Data Breach); and

(b) provide the Customer without undue delay (wherever possible, no later than 12 hours after notifying the Customer under 1.14.1(a) of the Personal Data Breach) with such details as the Customer reasonably requires regarding:

(i) the nature of the Personal Data Breach, including the categories and approximate numbers of Data Subjects and Personal Data records concerned; and

(ii) any investigations into such Personal Data Breach; and

(iii) the likely consequences of the Personal Data Breach; and

(iv) any measures taken, or that Dataflow recommends, to address the Personal Data Breach, including to mitigate its possible adverse effects,

provided that, (without prejudice to the above obligations) if Dataflow cannot provide all these details within such timeframes, it shall before the end of this timeframe, provide the Customer with reasons for the delay and when it expects to be able to provide the relevant details (which may be phased), and give the Customer regular updates on these matters.

1.14.2 Each party shall promptly (and in any event within three Business Days) inform the other if it receives a Complaint which is directly relevant to the Service provided under this Addendum and provide the other party with full details of such Complaint.

1.15 **Deletion or return of Protected Data and copies**

1.15.1 Dataflow shall without delay, at the Customer's written request, either securely delete or securely return all the Protected Data to the Customer after the end of the provision of the relevant Services related to processing or, if earlier, as soon as processing by Dataflow of any Protected Data is no longer required for the purpose of Dataflow's performance of its relevant obligations under the Agreement, and securely delete existing copies (unless storage of any data is required by Applicable Law and, if so, Dataflow shall inform the Customer of any such requirement).

1.16 **Liability and indemnities**

1.16.1 Neither Party excludes or limits its liability in respect of the terms of this Addendum.

1.16.2 This Addendum is intended by the Parties to be supplemental to and be read in conjunction with any provisions in the Agreement (or in any agreement) in relation to the liability of Dataflow to the Customer.

1.16.3 Dataflow shall indemnify and keep indemnified the Customer in respect of all DP Losses suffered or incurred by the Customer, arising from or in connection with:

(a) any breach by Dataflow of its obligations under this Addendum; and/or

(b) Dataflow acting outside or contrary to the lawful instructions of the Customer in respect of the processing of Protected Data.

1.16.4 Dataflow shall during the term of the Agreement and for three years thereafter and at its own cost effect and maintain in force with, appropriately regulated insurers of good financial standing and good repute in the international insurance market an insurance policy to insure against the risks and liabilities to which Dataflow is subject to under this Addendum (the **"Insurance"**).

1.16.5 Dataflow shall:

(a) administer and maintain the Insurance, and Dataflow's relationship with its insurers, at all times in accordance with Good Industry Practice so as to preserve their benefits and on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time; and

(b) do nothing to invalidate the Insurance or to prejudice Customer's entitlement thereunder; and

(c) make available to Customer, on reasonable notice, all relevant information to satisfy it that the Insurance is appropriate.

1.17 **Counterparts**

1.17.1 This Addendum may be executed and delivered in any number of counterparts, each of which is an original and which, together, have the same effect as if each Party had signed the same document. Transmission of an executed counterpart of this Addendum by email, shall take effect as delivery of an executed counterpart of this Addendum. No counterpart shall be effective until both Parties have executed and delivered at least one counterpart.

Appendix 1

Answers to GDPR Questionnaire and any supporting documentation

The “processing of data” is limited to storing a copy of your accounting database for a short period of time in order to provide support for Dataflow’s products to your finance department, or to test the implementation of new functionality in the software we provide for our clients.