DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**"), forms part of the Contract between Payroll Options Ltd (the "**Company"**) and the Client. All capitalised terms not defined in this DPA shall have the meanings set forth in the Contract. In the event of any conflict or discrepancy between the Terms and Conditions and this DPA, the Terms and Conditions shall prevail.

1) DEFINITIONS
   a) "**Client Data**" means any Personal Data that the Company processes on behalf of the Client as a Data Processor in the course of providing Services, as more particularly described in this DPA.
   b) "**Contract**" means the Company's Terms and Conditions (as updated by the Company from time to time), the Schedule of Services and Additional Charges and this DPA, which govern the provision of the Services to Client.
   c) "**Data Controller**" means an entity that determines the purposes and means of the processing of Personal Data, in this instance the Client.
   d) "**Data Processor**" means an entity that processes Personal Data on behalf of a Data Controller, in this instance the Company.
   e) "**Data Protection Laws**" means EU Data Protection Law and the UK Data Protection Law.
   f) "**EEA**" means, for the purposes of this DPA, the European Economic Area, United Kingdom and Switzerland.
   g) "**EU Data Protection Law**" means (i) Regulation 2016/679 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 (General Data Protection Regulation) ("**GDPR**"); and (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector and applicable national implementations of it (as may be amended, superseded or replaced).
   h) "**Personal Data**" means any information relating to an identified or identifiable natural person.
   i) "**Processing**" has the meaning given to it in the GDPR and "**process**", "**processes**" and "**processed**" shall be interpreted accordingly.
   j) "**Security Incident**" means any unauthorised or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Client Data.
   k) "**Services**" means the payroll service provided by the Company to the Client pursuant to the Contract.
   l) "**Sub-processor**" means any Data Processor engaged by the Client to assist in fulfilling its obligations with respect to providing the Services pursuant to the Contract or this DPA. Sub-processors may include third parties.
   m) "**Terms and Conditions**" means the Company's terms and conditions as published on their website from time to time.
   n) "**UK Data Protection Law**" means the Data Protection Act 1998, or any superseding act.
2) RELATIONSHIP WITH THE CONTRACT
   a) The parties agree that this DPA shall replace any existing DPA the parties may have previously entered into in connection with the Services.
   b) If there is any conflict between this DPA and the Terms and Conditions, this DPA shall prevail to the extent that the conflict applies to data protection.

c) Any claims brought under or in connection with this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Contract.

d) Any claims against the Company under this DPA shall be brought solely against the entity that is a party to the Contract. In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise. The Client further agrees that any regulatory penalties incurred by the Company in relation to the Client Data that arise as a result of, or in connection with, the Client's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce the Company's liability under the Contract as if it were liability to the Client under the Contract.

e) This DPA may be updated as and when required by the Company, by posting the revised version on the Company's website (https://PayrollOptions.com/DataProcessingAddendum) which shall become effective at the time of posting.

f) This DPA shall be governed by and construed in accordance with the laws of England and Wales.

3) SCOPE AND APPLICABILITY OF THIS DPA

a) This DPA applies where and only to the extent that the Company processes Client Data that originates from the EEA and/or that is otherwise subject to EU Data Protection Law on behalf of the Client as **Data Processor** in the course of providing Services pursuant to the Contract.

4) ROLES AND SCOPE OF PROCESSING

a) **Role of the Parties.** As between the Company and the Client, the Client is the **Data Controller** of Client Data, and the Company shall process Client Data only as a **Data Processor** acting on behalf of the Client.

b) **Client Processing of Client Data.** The Client agrees that (i) it shall comply with its obligations as a Data Controller under Data Protection Laws in respect of its processing of Client Data and any processing instructions it issues to the Company; and (ii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under Data Protection Laws for the Company to process Client Data and provide the Services pursuant to the Contract and this DPA.

c) **Company Processing of Client Data**. The Company shall process Client Data only for the purposes described in this DPA and only in accordance with the Client's documented lawful instructions. The parties agree that this DPA and the Contract set out the Client's complete and final instructions to the Company in relation to the processing of Client Data and processing outside the scope of these instructions (if any) shall require prior written agreement between the Client and the Company.

d) **Details of Data Processing.**

i) Subject matter: The subject matter of the data processing under this DPA is the Client Data.

ii) Duration: As between the Company and the Client, the duration of the data processing under this DPA is until the termination of the Contract in accordance with the Company's Terms and Conditions.

iii) Purpose: The purpose of the data processing under this DPA is the provision of the Services to the Client and the performance of the Company's obligations under the Contract (including this DPA) or as otherwise agreed by the parties.

iv) Nature of the processing: The Company provides Payroll Services, as described in the Contract.

v) Categories of data subjects: The Company processes payroll data concerning the Client's employees.

e) **Types of Client Data:**

i) Client employee data: Information required to accurately calculate Gross Pay, PAYE Tax, National Insurance and statutory absence payments in accordance with HMRC requirements. Further information to calculate pension contributions, attachment of earnings and additional payments and deductions (including union deductions). Required information will include: Full name, address, date of birth, NI Number, salary details, hours worked per week, start date, Tax Code, NI Category.

Further information may be required for optional services such as bank details and email address. From this information further values are derived/calculated to enable the appropriate statutory deductions to be calculated accurately.

5) SUBPROCESSING

a) Authorised Sub-processors. The Client agrees that the Company may engage Sub-processors to process Client Data on the Client's behalf. The Sub-processors currently engaged by the Company and authorised by the Client are listed in Annex A.

b) **Sub-processor Obligations.** The Company shall: (i) where possible enter into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Client Data to the standard required by Data Protection Laws; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause the Company to breach any of its obligations under this DPA.

6) SECURITY

a) **Security Measures**. The Company shall implement and maintain appropriate technical and organisational security measures ("**Security Measures**") to protect Client Data from Security Incidents and to preserve the security and confidentiality of the Client Data in accordance with the Company's security standards audited and approved by Payment Services UK.

b) **Updates to Security Measures**. The Client is responsible for reviewing the information made available by the Company relating to data security and making an independent determination as to whether the Services meet the Client's requirements and legal obligations under Data Protection Laws. The Client acknowledges that the Security Measures are subject to technical progress and development and that the Company may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Client.

c) **Client Responsibilities.** Notwithstanding the above, the Client agrees that except as provided by this DPA, the Client is responsible for its secure use of the Services, protecting the security of Client Data when in transit to and from the Company and taking any appropriate steps to securely encrypt or backup any Client Data uploaded or emailed to the Company.

i) As the Data Controller the Client accepts responsibility for all information posted by the Company to the Client. In the instance of Royal Mail First Class Post being the delivery method for any payroll information, the client will review and consider whether appropriate security measures are in place with Royal Mail First Class Post and decide if the following services are required at an additional cost:

(1) Delivery by Royal Mail Special Delivery

(2) Online Payslips

7) SECURITY REPORTS AND AUDITS

a) The Client acknowledges that the Company is audited by Payment Services UK as part of the BACS Approved Bureau Scheme. This audit covers the following areas (references to our/we mean Payroll Options Ltd):

Organisation and policy	This section covers organisation, policies and issues of security and control, to identify organisations whose areas of responsibility are well defined and adequately resourced with proper attention paid to personnel, security and control issues.
Financial Information	The purpose of this section is to obtain financial information regarding our business and holding companies

Commercial Arrangements	This section examines our relationship with our clients/customers to establish that responsibilities and liabilities are clearly defined.
Professional Services	This section gathers information about the services that we provide, to enable us to assess the risk associated with our BACS business.
Physical Security	This section covers the physical security of our bureau operations, to establish that access to them is well controlled and that they are properly protected from hazards such as fire, flood or malicious damage.
Computer Facilities and Networks	Information about our computer facilities and networks.
Logical Access Control	This section is designed to ensure that use of the BACS applications is restricted to authorised users only. To enforce good security disciplines and procedures, with emphasis on passwords, network control and compliance checks.
Computer Operations	In this section our computer operations are examined to verify that operators have adequate instructions and support, and that storage media are properly handled, so that unexpected problems can be managed with the minimum impact.
Business Continuity	This section examines how we would cope if an incident ranging from a minor failure to a major systems problem or a disaster, such as fire or flood, were to affect our operations. To identify that we can show we have considered all aspects of, and demonstrated our ability to cope with such a situation.
Applications and Systems Support	This section seeks to establish that there are appropriate controls over the computer and network operating systems and other systems software to minimise the risk of disruption.
Customer Data Controls	This section addresses the process for handling BACS client/customer data and the controls that ensure that it is properly processed and checked to protect against potential fraud.
Production of BACS Data	This section covers the controls over the production of BACS data.
BACStel-IP Transmission Controls	This section examines how our organisation uses the controls BACStel-IP provides to ensure the secure transfer of data to the BACS clearing.
Verification of BACS Processing	Various BACS reconciliation reports are produced to verify that client/customer data has been processed accurately. This section looks at how the reports are used and at the procedures for reconciling the reports and resolving any problems in a timely manner.

b) The Company shall provide when requested a summary document in respect of information security. In the event that further information is required which is not contained within this summary document the Company shall provide written responses to reasonable further requests for information made by the Client that are necessary to confirm the Company's compliance with this DPA, provided that the Client shall not exercise this right more than once per year.

8) DATA LOCATIONS

a) **Data centre location**. The Company's data centres are located in the United Kingdom. The Company shall at all times provide an adequate level of protection for the Client Data processed, in accordance with the requirements of Data Protection Laws.

9) ADDITIONAL SECURITY

a) **Confidentiality of processing.** The Company shall ensure that any person who is authorised by the Company to process Client Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

b) **Security Incident Response**. Upon becoming aware of a Security Incident, the Company shall notify the Client without undue delay and shall provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by the Client.

c) **Staff Training**. Employees of the Company will be trained in data protection and specifically in awareness of GDPR at a level suitable for their job role.

10) CHANGES TO SUB-PROCESSORS

a) Annex A listing sub-processors may be updated as and when required by the Company by posting the revised version on the Company's website https://PayrollOptions.com/DataProcessingAddendum

b) The Company will notify the Client (for which email shall suffice) if it adds or removes Sub-processors

c) The Client may object in writing to the Company's appointment of a new Sub-processor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties shall discuss such concerns in good faith with a view to achieving resolution. If this is not possible, the Client may suspend or terminate the Contract (without prejudice to any fees incurred by the Client prior to suspension or termination).

11) DELETION OF DATA

a) Upon termination of the Contract, the Company will delete all active payroll data relating to the Client in its possession or control within 3 months of the final pay date, save that this requirement shall not apply to the extent the Company is required by applicable law to retain some or all of the Client Data, or to Client Data it has archived on back-up systems, which Client Data the Company shall securely isolate and protect from any further processing, except to the extent required by applicable law.

b) For clients that we provide online payslips, the client will be given the option to extend this service for an additional fee in accordance with the Schedule of Services and Additional Charges, for a period of 3, 6 or 12 months, within one month of the end of this service the online payslip data for that company will be deleted.

12) COOPERATION

a) The Services provides the Client with Client Data which the Client may use to assist it in connection with its obligations under the GDPR, including its obligations relating to responding to requests from data subjects or applicable data protection authorities. If the Client is unable to access the relevant Client Data, the Company shall (at the Client's expense) provide reasonable assistance to the Client to respond to any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Contract. In the event that any such request is made directly to the Company, the Company shall not respond to such communication directly without the Client's prior authorisation, unless legally compelled to do so. If the Company is required to respond to such a request, the Company shall promptly notify the Client and provide it with a copy of the request unless legally prohibited from doing so.

b) If a law enforcement agency sends the Company a demand for the Client Data (for example, through a subpoena or court order), the Company shall attempt to redirect the law enforcement agency to request that data directly from the Client. As part of this effort, the Company may provide the Client's basic contact information to the law enforcement agency. If compelled to disclose the Client Data to a law enforcement agency, then the Company shall give the Client reasonable notice of the demand to allow

the Client to seek a protective order or other appropriate remedy unless the Company is legally prohibited from doing so.

c) To the extent the Company is required under Data Protection Law, the Company shall (at the Client's expense) provide reasonably requested information regarding the Services to enable the Client to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

Annex A - List of the Company's Sub-processors

The Company uses a small number of third-party Sub-processors to assist it in providing the Services. These Sub-processors provide storage services, email, cloud hosting, payment services and online payslip services.

Entity Name	Location	Service Provided
Sweep Limited, trading as ePayslips.co.uk	Grimsby, United Kingdom	Online Payslip Service
Lloyds Bank (BACS sponsor for Payroll Options Ltd)	London, United Kingdom	Payment Services
Microsoft	United Kingdom (Reading, Edinburgh, Manchester, Cambridge, London)	Cloud Hosting, Storage Services and Email
Alphabet Inc. (Google)	London, United Kingdom	Storage Services for Finance Department
PensionSync ltd	London, United Kingdom	Pension Upload Automation Service
iVoxx	London, United Kingdom	Phone Services
Mailgun Technologies inc.	Frankfurt, Germany	Transactional Email Service

Last updated January 2024