RollPay Bureau Limited - Data Processing Agreement
(21st March 2018)

This agreement and its associated schedules shall come into force with effect from 25th May 2018 and shall from that date replace any previous terms with the header 'Data Protection' (Section 5,7 or otherwise) and work in addition to section 7 of the current full RollPay Terms of Business 2018.

1. This section on data processing (the "Data Processing Agreement") specifies the data protection obligations of the Parties which arise in connection with the provision of the Services under this Order. This Data Processing Agreement applies to all activities performed in connection with this Order in which Processor and, if and insofar permissible, a third party acting on behalf of Processor may come into contact with personal data belonging to the Controller.
2. The relevant types of personal data, the individuals these personal data refer to and the types of processing of personal data being undertaken are dependent on the products and services purchased by the Client under this Order and are set out at Appendix 1.
3. The term of this Data Processing Agreement is equal to the term of the Order. Clauses 32 and 33 of this document set out the position of the parties at the end of the term.
4. For the purposes of this Data Processing Agreement, both parties hereby acknowledge and confirm that the Employer is the Data Controller, (hereinafter "Controller") and RollPay is the Data Processor, (hereinafter "Processor"). It is agreed that where a Client is not the Data Controller the Client makes this agreement on behalf of the Data Controller and have the relevant written authority to do so.

Definitions

5. "Data Protection Legislation" means the EU General Data Protection Regulation (effective 25th May 2018) and all other applicable laws and regulations relating to the processing of personal data and privacy.
6. "Personal Data" means any information relating to an identified or identifiable natural individual as defined by applicable Data Protection Legislation.
7. "Processing" means processing of Personal Data on behalf of Controller as defined by applicable Data Protection Legislation.
8. "Instruction" means a written instruction, issued by Controller to Processor, and directing Processor to perform a specific action with regard to Personal Data. These instructions may from time to time or case to case thereafter, be amended, amplified or replaced by Controller in separate written instructions.

   Scope and responsibility
9. Both parties shall assist each other in complying with its applicable obligations under the Data Protection Legislation. Each Party shall at all times comply with the Data Privacy Applicable laws and Regulatory Requirements with regards to the provision of the Services under this Order and shall under no circumstances make the other Party in breach of these laws, rules or regulations.
10. Processor shall Process Personal Data on behalf of Controller and always in accordance with the Data Protection Legislation and codes of practice applying to the Processor.

Obligations of Processor

11. Processor shall process Personal Data only within the scope of Controller's Instructions. Processors interpretation of those instructions in so far as it applies to the products and services specified on this Order form can be found at Appendex 1. Controller hereby acknowledges that the processing specified in Appendix 1 comprise its instructions to the Processor. If Processor is required to process the Personal Data for any other purpose by applicable law, Processor will inform the Controller of this legal requirement, to the extent permitted to do so by the applicable law. Processor shall not process Personal Data for its own purposes and shall keep Controller' Personal Data logically separate to data processed on behalf of any third party.
12. Processor shall notify Controller immediately if, in Processor's reasonable opinion, an Instruction breaches the Data Protection Legislation.
13. Processor shall take appropriate technical and organizational measures to adequately protect Controller's Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure taking into account the nature of the Processing, The Controller acknowledges that the technical and organizational measures set out in the above link are subject to technical progress and development. Processor may implement, without advance notification to The Controller, adequate alternative measures providing these are no less adequate than the level of security provided by the specified measures accepted by Controller at the time of signing this Order

Form. Any adequate alternative measures shall be updated at the above link from the time they are implemented.

14. If Processor becomes aware of known or suspected breaches of security leading to or which may have led to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data that Processor has processed ("Personal Data Breach"), Processor shall provide Controller with a description of the Personal Data Breach, the types of data that was the subject of the Personal Data Breach and the identity of each affected person as soon as such information can be collected or otherwise becomes available, as well as any other information Controller may reasonably request relating to the Personal Data Breach. In the event of a Personal Data Breach, Processor will without undue delay (i) take action immediately to investigate the Personal Data Breach and to identify, prevent recurrence and make reasonable efforts to mitigate the effects of any such Personal Data Breach and (ii) to carry out any recovery or other action necessary to remedy the Personal Data Breach. Processor shall not release or publish any filing, communication, notice, press release or report concerning any Personal Data Breach in respect of Controller's Personal Data without Controller's prior written approval.
15. Controller agrees that an unsuccessful security incident will not be subject to disclosure as per clause 14. An unsuccessful security incident is one that does not lead to any unauthorised access to Personal Data of the Controller or to any of the hardware or facilities of the Processor used for storing Personal Data of the Controller. This includes but is not limited to port scans, denial of service attacks, pings and other such broadcast attacks on firewalls and unsuccessful log-on attempts.
16. The Processor shall ensure that all personnel who have access to Personal Data belonging to Controller under the terms of this Data Processing Agreement maintain confidentiality, and that such obligations are contractually imposed. Processor shall ensure that access to Controller's Personal Data is limited to those persons who need access in order to meet the Processor's obligations under this Data Processing Agreement and that such access is only granted to such parts of the Controller's Personal Data as is strictly necessary in relation to that person's particular duties. Processor shall ensure that all personnel who have access to the Personal Data have undertaken training appropriate to their role in relation to the handling of Personal Data and applicable Data Protection Legislation.
17. Processor shall maintain descriptions of all Personal Data Processing activities carried out on behalf of Controller containing the information prescribed in applicable Data Protection Legislation (including but not limited to the type of Personal Data Processed and the purposes for which they are processed). The Processor has made these documents available at Appendix 1.
18. Processor will immediately notify Controller of any monitoring, auditing or control activities and measures undertaken by a supervisory authority where Processor is permitted to do so by such supervisory authority.
19. The Personal Data will be processed and used by Processor exclusively within the territory of a member state of the European Union or the European Economic Area. Any transfer of Personal Data to a third country outside of this area requires the prior written consent of Controller.
20. Processor acknowledges and agrees that all rights, title and interest in Controller's Personal Data (including all intellectual property rights subsisting therein) shall vest solely in Controller.
21. Processor shall, upon request, permit a supervisory authority to access its premises, computer and other information systems, records, documents and records (where permitted by applicable Data Protection Legislation) to enable the supervisory authority to satisfy themselves that Processor is complying with its obligations under this Data Processing Agreement and applicable Data Protection Legislation.
22. During the term of the Order the Controller is authorised to audit the technical and organisational measures taken by the processor (hereinafter “Audit”) in order to ensure Processor complies with its obligations under this Data Processing Agreement. Where Controller intends to conduct such an audit of the Processor it shall provide the latter with prior written notice a minimum of ten (10) working days before the beginning of the audit. All audits shall be defined by the Controller, who shall be responsible for all costs. Audits may be carried out by (i) Controllers suitably qualified employees, (ii) External auditors of the Controller, (iii) regulators of the Controller, (iv) independent consultants appointed by the Controller and /or (v) voluntary disclosures from the Processor. Should the Controller wish the audit to be performed by an external auditor or an independent consultant, the Controller must inform the Processor to allow it to raise the potential situation of conflicts of interest with the proposed external auditor or independent Consultant. The absence of an issue raised by Processor within 5 days following the date of notice will amount to a tacit approval. During the audit, Processor will provide with no undue delay information, reasonable assistance and access to its premises as may be necessary in order that those conducting the audit may fully and promptly carry out each audit. The controller acknowledges that due to security constraints physical access to the subcontracted hosting facilities may not be possible and this will not be considered a breach of the Controllers right to audit.

Obligations of Controller

23. Controller and Processor shall each be responsible for complying with their applicable obligations under the Data Protection Legislation.
24. Controller is responsible for securing data subject's rights. Processor shall assist Controller in securing such rights.
25. Any additional reasonable costs arising in connection with the return or deletion of Personal Data after the termination or expiration of this Order shall be borne by Controller.
26. Controller is solely responsible for securing a legitimate legal basis for processing of the Personal Data in respect of the Personal Data it collects and requires the Processor to Process. Controller hereby indemnifies Processor against all claims, and other applicable actions brought by any Data Subject/s where Controller has failed to have a legitimate legal basis for the processing of the Personal Data that it requires Processor to carry out. Enquiries by Data Subjects to Controller
27. Where Controller is obliged, under the Data Protection Legislation, to provide information to an individual or a government, regulatory or supervisory authority about the Processing of his or her Personal Data, Processor shall assist Controller in making this information available promptly and no later than 10 working days from receipt of such written request from the Controller.
28. If a data subject should apply directly to Processor to request access to, or the rectification, erasure, restriction or portability of, his personal data, or to object to the Processing of his Personal Data, Processor will forward this request to Controller without delay and no later than 5 working days after receipt. Processor will only correct, delete or block the Personal Data Processed on behalf of Controller when instructed to do so in writing by the Controller. Subcontractors
29. The engagement of subcontractors by Processor requires Controller's consent. In agreeing the RollPay Terms of Business Controller hereby gives consent to Processor to use subcontractors. Having regard to clauses 30 and 31 below Controller acknowledges that the subcontractors may be changed from time to time without prior notice being given by the processor.
30. Where Processor engages subcontractors with consent of Controller, Processor shall contractually require such subcontractors to comply with obligations that are substantially similar to those set forth herein, including in particular, but not limited to, the contractual requirements for confidentiality, data protection and data security. Processor shall restrict subcontractor's access to Personal Data of the Controller to the extent necessary for them to provide their services.
31. For the avoidance of doubt, where a subcontractor fails to fulfil its obligations under any subprocessing agreement, Processor will remain fully liable to Controller for the fulfilment of its obligations under this Data Processing Agreement. Deletion and/or return of data and data retention
32. Within 14 calendar days of the contract end date or upon written request from the Controller if earlier Processor will delete the Personal Data of the Controller in compliance with the Data Protection Legislation. A deletion log will be created and made available on request.
33. Whilst the controller maintains a contractual relationship with the Processor and utilises the products and / or services of the Processor the Processor will retain the data of the Controller as set out in the Retention of Record Policy (RRP) unless the Controller makes a written request for an alternative data retention period.

    Processor will not retain data of the Controller for longer than the maximum period shown in any event.
    Both Controller and Processor agree that Processor will retain Controller data for a maximum of 15 days following the end of a contract period (the Grace Period) where no renewal contract has been agreed between the parties prior to that end date. On the expiry of the Grace Period Processor will delete all Controller data.

    Where Controller use multiple products of Processor and the contract periods relating to each are not co-terminus Processor will only delete the Controller account on the expiry of the latest end date in those contracts, in the intervening period Processor will suspend Controller access to the products where contracts have expired. Duties to Inform, Mandatory Written Form

34. In the event that Processor (i) is required by law, court order, warrant, subpoena, or other legal judicial process to disclose any of Controller's Personal Data to any person other than Controller or (ii) receives any inquiry, communication, request or complaint from any governmental, regulatory or supervisory authority, Processor shall, where legally permitted to do so, immediately notify Controller in writing and shall furnish all reasonable assistance in a timely manner to Controller to enable it to respond or object to, or challenge any such inquiries, communications, requests, or complaints and to meet applicable statutory or regulatory deadlines.

35. No change of or amendment to this Data Processing Agreement or any of its requirements, including any commitment issued by Processor, shall be valid and binding unless made in writing and unless they make express reference to being a change or amendment to this Data Processing Agreement. Any waiver of any provision of this Data Processing Agreement shall be recorded in written form.

Appendix 1: Table of data

This Appendix only covers the processing of personal data as defined by the General Data Processing Regulation. The activities have been summarised at a service level and apply if you have purchased those services from us. Where you have purchased one or more of our services we consider the information shown to be your written instructions to us to perform the actions listed in accordance with the General Data Protection Regulation. This document may be updated from time to time as and when new features, functionality or products and services are released that involve the processing of personal data belonging to a Client or Employer. RollPay is under no obligation to provide notice of any changes or updates.

Services	Data type	File Type
Payroll only service Auto enrolment 'AE' (Full Setup) Auto Enrolment 'AE' (ongoing) Pension provider upload/data sync Declaration of compliance Pension (non AE) Virtual Service Initial data conversion	Name & Surname, Email Address, Home Address, Postcode, Mobile Phone, Home Phone, Date of birth, Citizenship, Gender, Current Job Title, Current Employer, Length at Employer, Education History, Skills, Desired Salary, Notice Period, Recruitment Status, Pay History, Flagging History, Unstructured CV, Qualifications, Communications (emails)	Payroll data file
Services	**Actions**	
Payroll only service Auto enrolment 'AE' (Full Setup) Auto Enrolment 'AE' (ongoing) Pension provider upload/data sync Declaration of compliance Pension (non AE) Virtual Service Initial data conversion	Add new and maintain employee data held within the payroll data file Process and calculate pay Process and calculate pension calculations Process Attachment of Earnings Orders Report to HMRC liabilities and perform EPS/FPS Keep employee and employer pension scheme records up to date Setup and provide a payroll portal service where required Provide help-desk support to an employers employees Keep Department of Work & Pensions up to date with employee records Liaise and make available employee data under legislation such as Child Maintenance Service, Court Orders and any other legal or regulatory requirements. Make BACS and Autopay transactions to pay employee wages where required	