## **DATA PROCESSING AGREEMENT**

**THIS AGREEMENT** is made [DATE]

# BETWEEN:

1. [NAME AND ADDRESS OF CLIENT] (the “Controller”); and,
2. HRinPractice Ltd., Astra House, The Common, Cranleigh, Surrey, GU6 8RZ, (the “Processor”).

# BACKGROUND

1. The Controller processes Personal Data in connection with its business activities;
2. The Processor processes Personal Data on behalf of other businesses and organisations;
3. The Controller wishes to engage the services of the Processor to process personal data on its behalf as defined in Schedule 2;
4. Article 17(2) of the Data Protection Directive 95/46/EC provides that, where processing of personal data is carried out by a processor on behalf of a data controller the controller must choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures;
5. Articles 17(3) and 17(4) of the Data Protection Directive require that where processing is carried out by a processor on behalf of a controller such processing shall be governed by a contract or legal act binding the processor to the controller stipulating, in particular, that the processor shall act only on instructions from the controller and shall comply with the technical and organisational measures required under the appropriate national law to protect personal data against accidental or unlawful destruction or accidental loss, alternation, unauthorised disclosure or access and against all other unlawful forms of processing;
6. In compliance with the above-mentioned provisions of Article 17 of the Data Protection Directive the Controller and Processor wish to enter into this processing security Agreement.

# THE PARTIES MUTUALLY AGREE AS FOLLOWS:

# 1. DEFINITIONS AND INTERPRETATION

1.1 In this Agreement the following words and phrases shall have the following meanings, unless inconsistent with the context or as otherwise specified:

“**Data Protection Directive**” shall mean Directive 95/46/EC of the European Parliament and Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

“**personal data**” shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic cultural or social identity;

“**processing of personal data**” shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

“**sub-contract**” and “**sub-contracting**” shall mean the process by which either party arranges for a third party to carry out its obligations under this Agreement and “Sub Contractor” shall mean the party to whom the obligations are subcontracted; and,

“**Technical and organisational security measures**” shall mean measures to protect personal data against accidental or unlawful destruction or accidental loss, alternation, unauthorised disclosure or access and against all other unlawful forms of processing.

# 2. CONSIDERATION

2.1In consideration of the Controller engaging the services of the processor to process personal data on its behalf the Processor shall comply with the security, confidentiality and other obligations imposed on it under this Agreement.

# 3. SECURITY OBLIGATIONS OF THE PROCESSOR

3.1 The Processor shall only carry out those actions in respect of the personal data processed on behalf of the Controller as are expressly authorised by the Controller.

3.2The Processor shall take such Technical and Organisational Security Measures as are required to protect personal data processed by the Processor on behalf of the Controller against unlawful forms of processing. Such Technical and Organisational measures shall include, as a minimum standard of protection, compliance with the legal and practical security requirements set out in Schedule 1 of this Agreement.

# 4. CONFIDENTIALITY

4.1 The Processor agrees that it shall maintain the personal data processed by the Processor on behalf of the Controller in confidence. In particular, the Processor agrees that, save with the prior written consent of the Controller, it shall not disclose any personal data supplied to the Processor by, for, or on behalf of, the Controller to any third party.

4.2 The Processor shall not make any use of any personal data supplied to it by the Controller otherwise than in connection with the provision of services to the Controller.

4.3 The obligations in clauses 4.1 and 4.2 above shall continue for a period of five years after the cessation of the provision of services by the Processor to the Controller.

4.4 Nothing in this agreement shall prevent either party from complying with any legal obligation imposed by a regulator or court. Both parties shall however, where possible, discuss together the appropriate response to any request from a regulator or court for disclosure of information.

# 5. SUB-CONTRACTING

**5.**1 The Processor may sub-contract its rights or obligations under this Agreement without the separate prior written consent of the Controller.

**5.2** Where the Processor, with the consent of the Controller, sub-contracts its obligations under this agreement it shall do so only by way of a written agreement with the Sub-Contractor which imposes the same obligations in relation to the security of the processing on the Sub-Contractor as are imposed on the Processor under this Agreement.

**5.3** For the avoidance of doubt, where the Sub-Contractor fails to fulfil its obligations under any sub processing agreement, the Processor shall remain fully liable to the Controller for the fulfilment of its obligations under this Agreement

# 6. TERM AND TERMINATION

**6.1** This Agreement shall continue in full force and effect for so long as the Processor is processing personal data on behalf of the Controller.

**6.2** Within 30 days following termination of this Agreement the Processor shall, at the direction of the Controller, (a) comply with any other agreement made between the parties concerning the return or destruction of data, or (b) return all personal data passed to the Processor by the Controller for processing, or (c) on receipt of instructions from the Controller, destroy all such data unless prohibited from doing so by any applicable law.

# 7. GOVERNING LAW

**7.1** This Agreement shall be governed by and construed in accordance with the laws of England and Wales.

**AS WITNESS** this Agreement has been signed on behalf of each of the parties by its duly authorised representative on the day and year first above written.

SIGNED on behalf of [NAME AND ADDRESS OF CLIENT]

………………………………………………………

(Authorised signatory)

[Name and title]

SIGNED on behalf of HRinPractice. Ltd.

………………………………………………………

Martin Evans, Director

# SCHEDULE 1

# Technical and Organisational Data Protection Measures

The following are the technical and organisational data protection measures referred to in Clause 3:

1. The Data Processor shall ensure that, in respect of all Personal Data it receives from or processes on behalf of the Data Controller, it maintains security measures to a standard appropriate to:
   * 1. the harm that might result from unlawful or unauthorised processing or accidental loss, damage, or destruction of the Personal Data; and
     2. the nature of the Personal Data.
2. In particular, the Data Processor shall:
   * 1. have in place, and comply with, a security policy which:
        + 1. defines security needs based on a risk assessment;
          2. allocates responsibility for implementing the policy to a specific individual
          3. is provided to the Data Controller on or before the commencement of this Agreement;
          4. is disseminated to all relevant staff; and
          5. provides a mechanism for feedback and review.
     2. ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in processing the Personal Data in accordance with best industry practice;
     3. prevent unauthorised access to the Personal Data;
     4. protect the Personal Data using pseudonymisation, where it is practical to do so;
     5. ensure that its storage of Personal Data conforms with best industry practice such that the media on which Personal Data is recorded (including paper records and records stored electronically) are stored in secure locations and access by personnel to Personal Data is strictly monitored and controlled;
     6. have secure methods in place for the transfer of Personal Data whether in physical form (for example, by using couriers rather than post) or electronic form (for example, by using encryption);
     7. password protect all computers and other devices on which Personal Data is stored, ensuring that all passwords are secure, and that passwords are not shared under any circumstances;
     8. take reasonable steps to ensure the reliability of personnel who have access to the Personal Data;
     9. have in place methods for detecting and dealing with breaches of security (including loss, damage, or destruction of Personal Data) including:
        + 1. the ability to identify which individuals have worked with specific Personal Data;
          2. having a proper procedure in place for investigating and remedying breaches of the GDPR; and,
          3. notifying the Data Controller as soon as any such security breach occurs.
     10. have a secure procedure for backing up all electronic Personal Data and storing back-ups separately from originals;
     11. have a secure method of disposal of unwanted Personal Data including for back-ups, disks, print-outs, and redundant equipment; and
     12. adopt such organisational, operational, and technological processes and procedures as are required to comply with the requirements of ISO/IEC 27001:2013, as appropriate to the Services provided to the Data Controller.

# SCHEDULE 2

# SERVICES

Provision of advice and guidance in relation to employment law compliance;

Provision of advice and guidance in relation to HR management, including performance, training, recruitment and employment benefits;

Provision of employment contracts and related material, policies and procedures, process workflows;

HR administration functions, excluding payroll processing;

Provision and administration of online HR management applications .

# SCHEDULE 3

# Personal Data

| **Type of Personal Data** | **Category of Data Subject** | **Nature of Processing Carried Out** | **Purpose(s) of Processing** | **Duration of Processing** |
| --- | --- | --- | --- | --- |
| Recruitment | Applicants for employment or other contracts for and of personal service | Collecting, analysing, reporting, creating legal and management documentation and providing advice | Advice and guidance on legal and contractual matters | 5 years |
| Contact | Employees, Directors, Partners, Trustees, workers and contractors | Collecting, analysing, reporting, creating legal and management documentation and providing advice | Advice and guidance on legal and contractual matters | 5 years |
| Terms and conditions of employment | Employees, Directors, Partners, Trustees, workers and contractors | Collecting, analysing, reporting, creating legal and management documentation and providing advice | Advice and guidance on legal and contractual matters | 5 years |
| Financial | Employees, Directors, Partners, Trustees, workers and contractors | Collecting, analysing, reporting, creating legal and management documentation and providing advice | Advice and guidance on legal and contractual matters | 5 years |
| Performance and conduct | Employees, Directors, Partners, Trustees, workers and contractors | Collecting, analysing, reporting, creating legal and management documentation and providing advice | Advice and guidance on legal and contractual matters | 5 years |
| Monitoring | Employees, Directors, Partners, Trustees, workers and contractors | Collecting, analysing, reporting, creating legal and management documentation and providing advice | Advice and guidance on legal and contractual matters | 5 years |
| Criminal offence | Employees, Directors, Partners, Trustees, workers and contractors | Collecting, analysing, reporting, creating legal and management documentation and providing advice | Advice and guidance on legal and contractual matters | 5 years |