

# Data Processing Agreement

This Agreement is made on

between

(1) [Client.FirstName] [Client.LastName] [Client.Company] hereby referred to as the Controller.

(2) Chronicle Computing Ltd hereby referred to as the Processor.  
(hereinafter referred to as the “Parties”)

## BACKGROUND:

- a) The Controller processes Personal Data in connection with its business activities;
- b) The Processor processes Personal Data on behalf of other businesses or organisations;
- c) The Controller wishes to engage the services of the Processor to process Personal Data on its behalf.

## DEFINITIONS AND INTERPRETATION

**Agreement:** this Data Processing Agreement.

**Business Day:** a day other than a Saturday, Sunday or public holiday in England when banks in London are open for business.

**Data Protection Authority:** the relevant data protection authority is the Information Commissioner Office (ICO)

**Data Protection Legislation:** means the Data Protection Act 2018 (DPA2018), United Kingdom General Data Protection Regulation (UK GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any legislation implemented in connection with the aforementioned legislation. Where data is processed by a controller or processor established in the European Union or comprises the data of people in the European Union, it also includes the EU General Data Protection Regulation (EU GDPR). This includes any replacement legislation coming into effect from time to time.

**Data Security Breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Shared Personal Data.

## SCOPE

The purpose of this Data Processing Agreement is to describe the work to be carried out by the Processor in relation with the Agreement. This Data Processing Agreement shall be deemed to take effect from the effective date and shall continue in full force and effect until termination of the Agreement.

## PROCESSING OF THE PERSONAL DATA

Customer is the Controller for the Personal Data and Chronicle Computing Ltd is the Processor for the Personal Data. The Processor agrees to process the Personal Data only in accordance with Data Protection Legislation.

Both Parties will comply with all applicable requirements of the Data Protection Legislation. This clause is in addition to, and does not relieve, remove or replace, a Party's obligations or rights under the Data Protection Legislation. In this clause 3, Applicable Laws means (for so long as and to the extent that they apply to either party) the law of the European Union, the law of any member state of the European Union and/or UK Law;

The Parties acknowledge that the Processor may process Personal Data on behalf of the Controller during the term of this Agreement. A description of the Personal Data and the processing activities undertaken by the Processor is set out in Appendix 1.

To the extent that the Processor processes Personal Data on behalf of the Controller in connection with this Agreement, the Processor shall:

Solely process the Personal Data for the purposes of fulfilling its obligations under this Agreement and in compliance with the Controller's written instructions as set out in this Agreement and as may be specified from time to time in writing by the Controller;

Notify the Controller immediately if any instructions of the Controller relating to the processing of Personal Data are unlawful;

Maintain a record of its processing activities in accordance with Article 30(1) of the GDPR;

Assist the Controller in ensuring compliance with the obligations set out in Articles 32 to 36 of the GDPR taking into account the nature of the data processing undertaken by the Processor and the information available to the Processor, including (without limitation):

### Sub-Processors

- a) The Controller gives the Processor general authorisation to replace any of its Sub-Processors or to add a new Sub-Processor. The Processor shall inform (by news article post on Chronicle Computing Website) the Controller of any intended changes concerning the addition or replacement of Sub-Processors.
- b) Ensure that obligations equivalent to the obligations set out in this clause 3 are included in all contracts between the Processor and permitted Sub-Contractors who will be processing Personal Data;
- c) Ensure that its Sub-Processor/Sub-Contractors shall not transfer to or access any Personal Data from a Country outside of the European Economic Area without the prior written consent of the Controller;

### **International Data Transfers**

The Processor shall comply with the Controller's instructions in relation to transfers of Personal Data to a Country outside of the European Economic Area unless the Processor is required, pursuant to Applicable Laws, to transfer Personal Data outside the European Economic Area, in which case the Processor shall inform the Controller in writing of the relevant legal requirement before any such transfer occurs, unless the relevant law prohibits such notification on important grounds of public interest;

### **Staff Confidentiality**

The Processor shall ensure that any persons used by the Processor to process Personal Data are subject to legally binding obligations of confidentiality in relation to the Personal Data and shall ensure that only such persons used by it to provide the Services have undergone training in Data Protection and in the care and handling of Personal Data;

### **Security Measures**

The Processor shall take appropriate technical and organisational measures against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of or damage to Personal Data taking into account the harm that might result from such unauthorised or unlawful processing, loss, destruction or damage and the nature of the Personal Data to be protected including without limitation, all such measures that may be required to ensure compliance with Article 32 of the GDPR;

### **Data Subject Rights**

- a) The Processor shall promptly notify the Controller if it receives a request from a Data Subject (Data Subject Access Request) under any Data Protection Legislation in respect of Personal Data; and
- b) Ensure that it does not respond to that request except on the documented instructions of the Controller or as required by applicable Data Protection Legislation to which the Processor is subject, in which case the Processor shall to the extent permitted by applicable Data Protection Legislation inform the Controller of that legal requirement before the Processor responds to the request; and
- c) Taking into account the nature of the data processing activities undertaken by the Processor, provide all possible assistance and co-operation (including without limitation putting in place appropriate technical and organisational measures) to enable the Controller to fulfil its obligations to respond to requests from individuals exercising their rights under the Data Protection Legislation;

### **Data Breaches**

The Processor shall provide information and assistance upon request to enable the Controller to notify Data Security Breaches to the Information Commissioner and / or to affected individuals and / or to any other regulators to whom the Controller is required to notify any Data Security Breaches;

### **Data Protection Impact Assessments**

The Processor shall provide input into and carry out Data Protection Impact Assessments in relation to the Processor's data processing activities;

### **Deletion Or Return Of Data**

- a) Upon termination of this Agreement, at the choice of the Controller, the Processor shall delete securely or return all Personal Data to the Controller and delete all existing copies of the Personal Data after a 6 months period unless and to the extent that the Processor is required to retain copies of the Personal Data in accordance with Applicable Laws in which case the Processor shall notify the Controller in writing of the Applicable Laws which require the Personal Data to be retained; and
- b) In the event that the Personal Data is deleted or destroyed by the Processor, the Processor shall provide the Controller with a certificate of destruction or written email confirming that the Personal Data has been destroyed or deleted;

### **Audits**

The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations set out in this clause 3 and allow for and contribute to audits, including inspections, conducted by or on behalf of the Controller or by the Information Commissioners Office (ICO) pursuant to Article 58(1) of the GDPR.

The Processor shall not transfer any Personal Data outside of the European Economic Area unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

- a) the Controller or the Processor has provided appropriate safeguards in relation to the transfer;
- b) the Data Subject has enforceable rights and effective legal remedies;
- c) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and
- d) the Processor complies with reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data.

## **GENERAL TERMS**

### **Indemnity**

The Processor provides no indemnity for the Controller against all costs, expenses (including legal and other professional fees and expenses), losses, damages, and other liabilities of whatever nature (whether contractual, tortious or otherwise) suffered or incurred by the Controller and arising out of or in connection with any breach by the Processor or any Sub-Contractors of this Agreement

### **Breach Identification And Notification**

The Processor shall notify the Controller without undue delay (and in any event within 24 hours) of becoming aware of a breach.

The Processor or any Sub-Contractor engaged by, or on behalf of, the Processor suffers a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data; or

The Processor or any Sub-Contractor engaged by, or on behalf of, the Processor receives any data security breach notification, complaint, notice or communication which relates directly or indirectly to the processing of the Personal Data or to either Party's compliance with the Data Protection Legislation. And in each case the Processor shall provide full co-operation, information and assistance to the Controller in relation to any such data security breach, compliance notice or communication.

### **Access**

Upon request the Processor shall allow the Controller, the ICO and its representatives access to the Processor's premises, records and personnel for the purposes of assessing the Processor's compliance with its obligations under this Agreement

### **Confidentiality**

Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law;

(b) the relevant information is already in the public domain.

## **GOVERNING LAW AND JURISDICTION**

This Agreement is governed by the laws of England and Wales. This Agreement, and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) is governed by and shall be construed and interpreted in accordance with the laws of England and Wales, and the Parties irrevocably submit to the exclusive jurisdiction of the Courts of England and Wales.

## **TERMINATION**

This Agreement may be terminated by the Controller giving not less than 6 months written notice to the Processor.

This Agreement may be terminated by the Processor giving not less than 6 months written notice to the Controller

On termination of this Agreement for whatever reason, the Processor shall cease to process the Personal Data and Confidential Information and shall arrange for the prompt and safe return of all of the Personal Data and Confidential Information, processed under the terms of this Agreement to the Controller, together with all copies of the Personal Data in its possession or control or that of its agents or contractors, within such time and by such secure means as the Controller shall provide for in writing at the time of termination of the Agreement.

On termination of this Agreement, should the Controller require the deletion of data still held by the Processor then the Processor is required to provide written evidence to support the deletion activity within the timeframe specified by the Controller.

Termination of this Agreement shall not affect any rights or obligations of either Party which have accrued prior to the date of termination and all provisions which are expressed to, or do by implication, survive the termination of this Agreement shall remain in full force and effect.

## NOTICES

All notices or other communications given to a Party under or in connection with this Agreement shall be in writing and shall be sent to the recipients set out below. Any notice may be delivered to the recipient personally, by first class post, recorded delivery or commercial courier at its registered office (if a company) or (in any other case) its principal place of business, or by facsimile. Any notice so served shall be deemed to have been delivered:

In the case of delivery by hand, when delivered;

In the case of facsimile, 12 hours after the time of confirmation of despatch;

If delivered by commercial courier, on the date and at the time that the courier's delivery receipt is signed;  
and

In the case of post or recorded delivery, at 9.00am on the second business day (or in the case of airmail 10 business days) after delivery to the postal authorities,

Provided that where, in the case of delivery by hand or by facsimile, such delivery or transmission occurs after 5.00pm on a business day or on a day which is not a business day, service shall be deemed to occur at 9am on the next following business day.

Either Party may from time to time change its address for notification purposes by giving the other written notice of the new address and the date upon which it will become effective.

AGREED by the Parties through their authorised signatories:

## **APPENDIX 1**

### **DATA PROCESSING ACTIVITIES**

#### **DESCRIPTION OF DATA**

This Appendix 1 includes the processing activities carried out by Chronicle Computing Ltd as required by Article 28(3) GDPR.

The data processed is as follows:

- Name
- Date of Birth
- Telephone Number
- Address
- Gender
- Religion
- Race
- National Insurance Number
- Payroll Number
- Pay Rate
- Hourly Rate
- Bonuses
- Adhoc Payments
- Contract of Employment
- Holiday Sick Absence Entitlement
- Appraisal Discipline Records
- Bank Account Details
- Next of Kin
- Medical Records
- Training and Skill record and documentation
- Email address personal and business
- IP address
- Precise location data

· Biometric Data – Facial image or Fingerprint Image

## CATEGORIES OF DATA SUBJECTS

The Controller has defined the following Data Subject categories from who the Personal Data as defined above will be collected.

- Employees
- Customers
- Contractors
- Visitors

## LAWFUL BASIS OF DATA PROCESSING

The Controller has determined the following lawful basis/bases to process personal data under the Data Protection Act 2018/GDPR 2016 is based on:

- Consent of the data subjects
- Contractual Obligation
- Legal Obligation
- Vital Interests
- Public Interest
- Legitimate Interests

## SPECIAL CONDITION OF PROCESSING SPECIAL CATEGORY DATA

The Controller has determined that the processing of special category personal data is based on the following special condition(s) under the Data Protection Act 2018/GDPR 2016:

- Explicit consent has been obtained from the data subject
- Processing is necessary in order to carry out obligations and exercise specific rights of the data controller for reasons related to employment, social security, and social protection
- Processing is necessary to protect the vital interests of data subjects where individuals are physically or legally incapable of giving consent
- Processing is necessary for the establishment, exercise, or defence of legal claims, for reasons of substantial public interest, or reasons of public interest in the area of public health
- For purposes of preventive or occupational medicine

- Processing is necessary for archiving purposes in the public interest, scientific, historical research, or statistical purposes
- Processing relates to personal data which are manifestly made public by the data subject
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects

## PROCESSING ACTIVITIES

The Company utilises the Sub-Contractors\* stated:

Provider	Data Subject Category	Data Held
Quickbooks – Accounting Software Pandadoc– Contract Management Software Stonly – Video and Support Content provider FlowRev – Defferred Revenue Software	Customer	Customer Address, Name
Zendesk – Support Ticketing System Pipedrive – Customer Relationship Management Software Microsoft Office – Word Excel PowerPoint Email Microsoft Azure – Data Hosting Provider Google Sheets – Data Collection Microsoft Teams – Online screenshare and meeting software Shape – UK Payroll Software HMRC Recognised	Customer/Employee/Visitor /Contractor	Customer Name, · Possibly Employees Name · Date of Birth · Telephone Number · Address · Gender · Religion · Race · National Insurance Number · Payroll Number · Pay Rate · Contract of Employment · Holiday Sick Absence Entitlement · Appraisal Discipline Records · Bank Account Details · Next of Kin · Medical Records · Training and Skill record and documentation · Email address personal and business · IP address · Precise location data · Biometric Data – Facial image or Fingerprint Image
ATS – US Hardware Manufacturer Grosvenor – UK Hardware Manufacturer		
Sysflex – External IT support to Chronicle and Access Control installation support Nuvemlogic – Azure data architecture and disaster recovery specialists.		

\*Where possible 2FA is used to access data in above platforms to enhance security and robustness. Minimal data is shared at all times.