Rushcliff Ltd

Data Processing Agreement

This Data Processing Agreement ("DPA") forms part of the main terms of use of PPS, PPS Express, PPS Online booking, any other Rushcliff products or services and the provision of support for Rushcliff products and services. This agreement is only valid and will only be legally binding upon acceptance of the main terms of use and when signed by an authorised agent of the customer.

How to execute this DPA:

1. This DPA consists of two parts: the main body of the DPA, and Appendices 1 and 2.
2. This DPA has been pre-signed on behalf of Rushcliff Ltd.
3. Complete the information in the signature box and sign on Page 8.

1. Definitions

The defined words here in quotes may be used in lower, upper or capitalised case in this document.
"Us" or "Our" or "we" refers to Rushcliff Ltd and any of our appointed agents.

"You" or "Your" refers to you and your organisation and staff as the client paying for or using PPS and our Support Services.

"PPS" is Private Practice Software as developed and produced by Rushcliff Ltd.

"the Services" means any products produced and maintained by Rushcliff Ltd including the provision of support for these products.

"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"GDPR" means the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data).

"Personal Data" refers to any information relating to an identified or identifiable natural person ('data subject') that is processed by us as a result of or in connection with the provision of the services under the main terms of use.

"Data Protection Laws" means any relevant laws including the GDPR and other UK laws governing the use of personal data.

"Data Controller" is the entity, organisation, other body or person that determines the purposes and means for the Processing of Personal Data. For the purposes of this agreement you are the Data Controller.

"Data Processor" means the entity that processes Personal Data on behalf of the Data Controller. For the purposes of this agreement Rushcliff is the Data Processor.

"Sub-Processor" means any third-party Processor appointed by us in provision of the Services that has, or may have, access to Personal Data.

A "Security Breach" is any accidental or unlawful access, alteration, destruction, loss of or loss of access to Personal Data. Loss of access will only be determined to constitute a Security Breach where access cannot be restored in a timely manner.

2. Processing of Personal Data

2.1 Roles of the parties
Both parties agree and acknowledge that with regard to the Processing of Personal Data you are the Data Controller and we are the Data Processor.

2.2 Your processing of personal data
You agree that you are responsible for determining the means and purpose of the Personal Data processing and, in your use of the Services, will guarantee that you process Personal Data in accordance the requirements of the GDPR and any other applicable data protection regulations including, but not limited to, ensuring the accuracy, quality and legality of the Personal Data processing and the means by which you acquired the Personal Data.

2.3 Our processing of personal data
We will treat and handle all Personal Data as confidential information. We will only process Personal Data on behalf of and in accordance with your documented instructions. This Data Processing Agreement details these instructions as processing for the following reasons: (i) Processing in relation to delivering and making available use of the Services. (ii) Processing for maintenance and support of the Services. (iii) Processing initiated by users in their use of the Services. (iv) Processing to comply with other written instructions by You where such instructions are consistent with this agreement and are determined by Us to be reasonable or are required under EU Data Protection Law.

We will not transfer, copy or otherwise process Personal Data in any way that is not detailed in the instructions we receive unless required to do so by relevant UK or EU Data Protection laws.

We will give notice to you, without undue delay, if at the time of receiving instructions relating to the Processing of Personal Data from you we consider them to be in conflict with the applicable Laws.

Where, and to the extent, that we process Personal Data as a controller, such as information that we process related to you for billing purposes, we will comply with applicable EU Data Protection laws in respect of that processing, as set out in our privacy policy. The terms of this agreement do not apply to any data Processing that we conduct as a Data Controller.

2.4 Details of the processing
The subject-matter and purpose of Personal Data processing by us is the provision of our Services to you and any other reasonable processing requests, received in writing and accepted by us or required by applicable law. The purpose, duration, categories of data subject and types of Personal Data processed under this DPA are further specified in appendix 1 of this agreement.

2.5 Data Transfers
All Personal Data processing conducted by Us or sub-processors that we engage with is conducted within the EU. We do not store any information in non-EU based systems and do not initiate transfer of any Personal Data to non EU countries.

The Services, either through cloud-based systems provided by us or by the PPS Sync service, may have the technical capability to be accessed or transfer Personal Data to countries outside the EU or third countries that the EU commission has determined to provide adequate protection to Data Subjects. Access to or transfer of data in this manner is not controlled or initiated by Us. Where you access or transfer Personal Data in this manner you are solely responsible for ensuring compliance with the relevant UK and EU Data Protection Laws including ensuring the Personal Data processing is only transferred where adequate safeguards are in place.

3. Rights of Data Subjects

3.1 Data Subject Request.
We will, to the extent permitted by law, notify you without undue delay if we receive a request from a data subject related to you under rights afforded to them by an applicable Data Protection Law. You agree that we will not respond directly to a data subject request without your prior written agreement other than to confirm that the request should be directed by the data subject to you. With your prior written consent we may respond directly at our discretion.

You agree that to the extent that you, in your use of the Services, do not have the ability to address a data subject request we shall, upon your request, provide reasonable assistance to facilitate the data subject's request to the extent that we are legally permitted and required to do so, provided that the data subject request is exercised in accordance with the relevant data protection laws. To the extent legally permitted you shall be responsible for any costs arising from our provision of such assistance. We shall be given reasonable time to assist with such requests and this assistance will not form or be regarded as part of the normal provision of support for the Services.

Where you are using an older, outdated or out of contract version of the Services it may not be possible for us to assist you and if you are using such an older, outdated or out of contract version of the Services we will not be obliged to provide assistance complying with the data subject request.

We shall not consider the use of an outdated version of the Services to constitute an inability to comply with a data subject request where a current version of the Services that would allow you to comply is available. In this situation we shall not be obliged to provide assistance in complying with the data subject request.

3.2 Timescales for complying with data subject requests
Where your use of the Services includes cloud-based Services, such as PPS Hosted or PPS Express, your database, including Personal Data, is automatically backed up as part of the provision of the Service. These backups are maintained for a maximum of 14 days, except where agreed in writing. You acknowledge and agree that in order to comply with data subject requests within the timescales required by the relevant laws any required action on your part must be undertaken no less than 14 days in advance of the deadline for complying with the request to the extent that such action is related to your use of the Services.

We are unable to access, alter or destroy individual pieces of data from within backups. If, following a data subject request under relevant UK or EU law, action has not been taken to comply with the request in sufficient time to ensure that no backup copy of the data exists contrary to the request, we will provide assistance by undertaking the removal of such backups in their entirety for the required days. You acknowledge and agree that to the extent legally permitted you shall be responsible for any costs arising from our provision of such assistance. We shall be given reasonable time to action such requests and this assistance will not form or be regarded as part of the normal provision of support for the Services.

4. Rushcliff Personnel

4.1 *Confidentiality.*
We ensure that all personnel involved in the Processing of Personal Data are informed of and understand the confidential nature of the Personal Data. All personnel operate under written confidentiality agreements that survive the termination of the personnel engagement.

We provide appropriate training to all personnel on their responsibilities and the handling of confidential information. The requirement for this and future training is reviewed regularly and additional training is provided as needed.

4.2 Limitation of access.
We ensure that access to Personal Data is limited to those personnel involved in processing the personal data in accordance with the instructions set out in this agreement and only to the extent that it is required for the specific processing activities that they are involved in.

5. Sub-Processors

5.*1 Use of Sub-Processors*
You acknowledge and agree that we may engage third-party sub-processors in connection with the provision, maintenance and development of the Services. In each case we have entered into a written agreement with the sub-processor detailing the processing activities and containing data protection obligations not less than those contained within this agreement to the extent applicable by the services provided by the third party.

5.2 List of Sub-Processors
We make available the current list of sub-processors for the Services. The list identifies each sub-processor that we engage with and the services they provide.

5.3 Changes to Sub-Processors
You acknowledge and agree that we may at times need to change or engage with additional sub-processors. We will notify you of changes or additions to the sub-processors that we engage with. You may object to the change of sub-processors by notifying us of your objection in writing within 14 days of the notice. In the event of an objection to a change of sub-processors we will take commercially reasonable steps to provide assurances or take action to ensure that the change is acceptable or to recommend an alternative configuration of Services that is not impacted by the change in sub-processors. If we are unable to take such action, provide assurances or recommend a change in configuration then you may terminate your agreement with us for the Services without penalty by providing written notification. You will be entitled to a refund for any prepaid fees for the Services.

6. Audit and Records

6.1 Records of Processing
We will, in accordance with UK and EU Data Protection Law, make available to you information in our possession or information reasonably required to detail our compliance with the obligations of a Data Processor under UK and EU Data Protection Law in relation to its processing of Personal Data. Such information includes records of processing activities completed in relation to our role as a Data Processor.

6.2 Audits

At least once every 18 months, we will conduct site audits of our Personal Data processing practices and the information technology and information security controls for all facilities and systems used in complying with our obligations under this Agreement, including, but not limited to, obtaining a network-level vulnerability assessment performed by a recognised third-party audit firm based on recognised industry best practices.

On your written request, we will make all of the relevant audit reports available to you for review. You will treat such audit reports as our confidential information under this Agreement.

We will promptly address any exceptions noted in the audit reports with the development and implementation of a corrective action plan by our management.”

7. Security

7.1 Security
We will maintain appropriate operational measures to ensure the security of all Personal Data that we Process. Such measures include, but are not limited to, the measures detailed in appendix 2.

We will undertake appropriate measures to ensure the security of Personal Data that we Process to the extent that we Process the Person Data, in particular protection against accidental or unlawful access, alteration, loss, disclosure or loss of access to Personal Data. Such measures include, but are not limited to, the measures detailed in appendix 2.

You acknowledge and agree that where you host and store your PPS database, such as when using a PPS Local system, You are responsible for the security of the stored Personal Data outside of the protection provided by the Services as detailed in appendix 2. You guarantee to undertake the appropriate technical and/or organisational measures required to ensure the security of the Personal data as required.

You acknowledge and agree that you are responsible for the technical security of any devices used to access the Services and indemnify Us of any liability for accidental or unlawful access, alteration, loss, disclosure or loss of access to of Personal Data arising from a lack of or failing of security applied to such devices.

You guarantee that your operational measures, including, but not limited to, those facilitated by features of the Services such as user access controls, as detailed in appendix 2, provide adequate protection to Personal Data to the extent that the Personal Data Processing is in relation to your use of the Services. You indemnify us of any liability for accidental or unlawful access, alteration, destruction, loss or loss of access to Personal Data arising from a lack of or failure of your implementation of operational measures.

8. Data Breach

8.1 Notification to You of Security Breaches
We will notify you without undue delay, and at the latest within 72 hours, of Us becoming aware of a breach of security leading to the accidental or unlawful access, alteration, destruction, loss or loss of access to Personal Data Processed by Us or any sub-processor that we engage with.

We will provide reasonable cooperation and assistance to You in respect of a security breach and provide you with all reasonable information in our possession concerning such a breach so far as the security breach affects you where relevant including, but not limited to, the possible cause and consequences of the security breach; the categories of Personal Data involved; a summary of any known unauthorised recipients of the Personal Data; measures taken by Us to mitigate any damage and prevent reoccurrence of the security breach.

8.2 Notification to Data Subjects of Security Breaches
Where a data breach must be reported to data subjects you agree and acknowledge that it is your responsibility to provide this notification to the data subjects and that we will not make any notification, unless required to do so by relevant UK or EU law, directly to data subjects.

8.3 Notification to other bodies of Security Breaches
You agree and acknowledge that where a security breach must be reported to the supervisory authority it is your responsibility to submit the notification of such a breach and that we will not, unless required to do so by UK or EU law, directly notify the supervisory body.

We will not, unless required by to do so by UK or EU law, make any public announcement about a security breach without your prior written consent.

9 General

9.1 Relationship to the main agreement
This DPA is without prejudice to the rights and obligations of the parties under the main agreement which shall continue in its entirety. In the event of any conflict between the terms of this agreement and the terms of the main agreement the terms of this agreement shall prevail as far as the matter concerns the Processing of Personal Data.

9.2 Limitation of liability
This Agreement shall not extend or further limit our liability to you other than as provided for in the main terms of use. Condition 11 of the main terms of use sets out our entire liability to you arising under or in connection with (i) the main terms of use and this Agreement; (ii) in respect of any use made by you of the Services or any part of them or with regard to our Processing of Personal Data under this Agreement; and (iii) in respect of any representation, statement or tortious act or omission (including negligence) arising under or in connection with the main terms of use or this Agreement.

For the avoidance of doubt, nothing in this Agreement or the main terms of use shall exclude our liability for:

a. death or personal injury caused by our negligence; or
b. fraud or fraudulent misrepresentation.

9.3 Obligation following termination of the main agreements
The parties agree that following the termination of the main agreement we will, at your choice, return the Personal Data in our standard format and destroy any instances of the Personal Data that we hold or destroy any instances of the Personal Data that we hold without return unless prevented by doing so by UK or EU law, in which case we guarantee not to continue Processing the Personal Data, except for storage and essential maintenance tasks and compliance with relevant UK or EU laws.

You agree that where, following the termination of the main agreement, you cannot be reached to provide a decision on the return of the Personal Data or cannot or will not provide access to a suitable device for us to return the Personal Data we will continue to store the Personal Data for a maximum of 30 days at which point all instances of the Personal Data in our possession will be destroyed, unless we are prevented from doing so by UK or EU law. In this situation Personal Data will only be retained past 30 days with your prior written agreement and then at our discretion.

You acknowledge and agree that where outstanding payments are due to Us we may, to the extent permitted by law, withhold return of the Personal Data until such time as all outstanding payments are received. Where the return of Personal Data is withheld whilst payments are outstanding we will continue to store the Personal Data for a maximum of 30 days at which point all instances of the Personal Data that we hold will be destroyed, unless we are prevented from doing so by UK or EU law. In this situation Personal Data will only be retained past 30 days with your prior written agreement and then at our discretion.

Data Protection Agreement Signature Page

The parties' authorised signatories have duly executed this DPA:

On behalf of Customer:

Business Name: _____

Name (written in full): _____

Position: _____

Address: _____

Signature: _____

Date: _____

On behalf of Rushcliff Ltd:

Name: John Upson

Position: Director

Address: Rushcliff Ltd, 1 Granary Wharf, Wetmore Road, Burton-on-Trent, Staffordshire, DE14 1DU.

Signature: DocuSigned by: _____ D70627003AAB4FD...

Date: 18/05/2018

Appendix 1

Nature and Purpose of Processing

We will process Personal Data as necessary to provide the Services detailed in this and the main agreement between you and us.

Duration of the Data Processing

We will process the personal data for the duration of this and the main agreement between you and us. Following the expiration or termination of the agreement we will, to the extent allowed by EU law stop the Personal Data Processing. We will return personal data to you in a method, format and time scale agreed by us.

Categories of Data Subjects

You may submit and process Personal Data using the services, the type and extent of which is solely controlled by you and which may include, but is not limited to, Personal and Special Data on the following categories of data subjects:

- Clients, customers, patients and contacts or representatives of these data subjects (who are natural persons).
- Employees or contractors of customers, clients, partners or suppliers to your organisation.
- Your employees, contractors, advisors and suppliers.
- Users that you authorise to use the Services (that are Natural Persons).

Types of Personal Data

The types and extent of personal data processed are solely controlled by you and may include, but are not limited to, the following types which include special categories of data:

- Names
- Title
- Date of Birth
- Sex
- Address
- Contact information
- Ethnic Origin
- Health or social care information
- ID information
- Personal life information
- Professional life information

Appendix 2

Security Measures

We and our sub-processors have implemented and maintain operational and technical security measures in accordance with industry standards and appropriate to the risks presented by the type and extent of the Personal Data Processed, supported by regular internal and external reviews. These security measures include those listed below. This is not an exhaustive list of all employed security measures.

Control of Physical Access

We and our sub-processors utilise suitable operational measures to ensure the physical security of sites that hold Personal Data and prevent physical access to hardware used for Personal Data Processing including application and database servers, network hardware and employee's workstations including:

- Control of physical access to Rushcliff premises, including visitor policies.
- Alarm, CCTV and other appropriate security measures in place at Rushcliff premises.
- Sub-processor data centres that host Personal Data are secure sites that maintain 24/7 on-site security, CCTV, motion tracking and logged internal smart access controls.

Access Controls for Data Processing Systems

We and our sub-processors employ appropriate measures to prevent Data Processing systems from being accessed or used by unauthorised individuals, including those inside and outside the organisation, including:

- Use of adequate encryption and other technologies to control access to workstations and applications involved in Personal Data Processing.
- Automatic locking of internal user accounts accessing workstations and database servers involved in the Processing of Personal Data following multiple incorrect password entries.

Access Controls for specific areas and activities of Data Processing Systems

We and our sub-processors commit to ensuring that personnel only have access to Personal Data as required to perform their responsibilities and authorised tasks and that personnel cannot access, read, copy, alter or destroy Personal Data without authorisation through various means including:

- Training and policies in respect of each individual's access rights to the Personal Data.
- Allocation of individual workstations and/or user accounts with access to Personal Data.
- Release of Personal Data only to authorised personnel including the allocation of differentiated programmatic access rights and roles controlling the data types individuals can access and the processing activities they can perform.
- On a database level data is stored in different normalised tables, separated by function and by data controller allowing data collected for different purposes to be processed individually.

Availability Control

Where your PPS Database is hosted by us, such as with PPS Hosted or PPS Express, suitable measures are maintained to ensure protection for Personal Data from accidental loss or destruction including;

- Redundant infrastructure allowing failure of individual components or systems without loss of data access.
- Managed, regular, automated backups of databases stored at a separate physical data centre and available for restore in the case of failure of the primary system. Daily backups are maintained and kept for a maximum of 14 days, allowing compliance with data subject rights requests under UK and EU law.
- Automated monitoring alerts technical and support personnel automatically of any issues or situations that may compromise availability of service.

Transmission Control

When data is transmitted or transferred through systems hosted by us, such as PPS Hosted, PPS Express and PPS Sync, or by our support or other authorised personnel in the completion of their duties we implement and maintain suitable measures to protect Personal Data from being accessed, read, copied, altered or destroyed by unauthorised parties during the transmission including:

- Use of adequate firewall and encryption technologies to protect the gateways and channels through which the data is transmitted.
- Use of adequate encryption technologies to protect the data in transit.
- Monitoring and alerts of incomplete data transfers.
- Logging of transfers and data transmission as far as is possible and relevant. Personal data itself is not included in transmission or transfer logs.

Security provisions provided by the services

We provide through the Services PPS Local and PPS Hosted, features to allow enforcement of your operational measures for Personal Data protection in respect to the principle of limitation of data access including:

- The ability to create an unlimited number of user accounts to ensure that each individual has their own account with unique login credentials.
- Functionality to set password complexity requirements for users.
- The ability, per user, to control the data processing activities that can be performed per data type within the Services including reading, alteration and destruction.