

## **PARTIES**

**This is an agreement between**

**Play Therapy (UK) – The United Kingdom society for Play and Creative Arts Therapies Limited (PTUK)** incorporated and registered in England and Wales with company number **04596316** whose registered office is at **The Coach House, Belmont Road, Uckfield East Sussex TN22 1BP (Processor)**

**And you the Therapist (user of Fortuna).**

### **BACKGROUND:**

**(A)** The Controller and the Processor entered into a **SERVICES AGREEMENT** for the use of Fortuna when you became a member of PTUK that may require the Processor to process Personal Data on behalf of the Controller.

**(B)** This Processor Agreement (**Agreement**) sets out the terms and conditions on which the Processor will process Personal Data when providing services under the Services Agreement. This Agreement contains the mandatory clauses required by Article 28(3) of the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (“UK GDPR”) (insofar as the UK GDPR applies) and Article 28(3) of the General Data Protection Regulation ((EU) 2016/679) (“EU GDPR”) (insofar as the EU GDPR applies) for contracts between controllers and processors.

### **AGREED TERMS:**

#### **1. DEFINITIONS AND INTERPRETATION**

The following definitions and rules of interpretation apply in this Agreement.

##### **1.1 Definitions:**

**Data Protection Legislation:** all applicable data protection laws in the UK and the EU including the UK GDPR, the Data Protection Act 2018 (and regulations made thereunder) (DPA 2018), the EU GDPR and any applicable national implementing laws, regulations and secondary legislation relating to the processing of Personal Data and the Privacy and Electronic Communications Directive (2002/58/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426).

**Data Subject:** an individual who is the subject of Personal Data.

**GDPR:** General Data Protection Regulation ((EU) 2016/679).

**Personal Data:** means any information relating to an identified or identifiable natural person that is processed by the Processor as a result of, or in connection with, the provision of the services under the Services Agreement; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**Personal Data Breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

**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.

**UK GDPR:** 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 as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act of 2018.

1.2 The Schedules form part of this Agreement and will have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Schedules.

1.3 A reference to writing or written includes email.

## **2. PROCESSING PURPOSES**

2.1 The Controller and the Processor acknowledge that the Controller is the controller and the Processor is the processor and that the Controller retains control of the Personal Data and remains responsible for its compliance obligations under Data Protection Legislation.

2.2. Where the Processor appoints a subcontractor pursuant to clause 4 below, the Processor shall be a data controller in relation to such processing.

2.3 The Processor may process the Personal Data categories and Data Subject types set out in Schedule 1 of this Agreement.

## **3. PROCESSOR'S OBLIGATIONS**

3.1 The Processor shall:

3.1.1 implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of Data Protection Legislation and ensure the protection of the rights of the Data Subject, as further set out below in this Agreement;

3.1.2 only use subcontractors to help with the processing of Personal Data in the circumstances set out in clause 4 below;

3.1.3 process the Personal Data only on documented instructions from the Controller, unless required to do so by Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

3.1.4 ensure that persons authorised to process the personal data (such as its employees) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

- 3.1.5 take the security measures set out in clause 5 below;
  - 3.1.6 taking into account the nature of the processing, assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights as set out in clause 6 below;
  - 3.1.7 assist the Controller in ensuring compliance with the obligations set out in clause 7 below (data breach) taking into account the nature of processing and the information available to the Processor;
  - 3.1.8 at the choice of the Controller, delete or return all the Personal Data to the Controller after the termination or expiry of the Services Agreement and delete existing copies (unless Union or Member State law requires storage of the Personal Data);
  - 3.1.9 make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of GDPR and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller;
  - 3.1.10 assist the Controller in ensuring compliance with the requirement to carry out Data Protection Impact Assessments as set out in Article 35 of GDPR, taking into account the nature of processing and the information available to the Processor;
  - 3.1.11 Designate a Data Protection Officer if required by Article 37(1) of GDPR and in accordance with the provisions of Articles 37, 38 and 39 of GDPR; and
  - 3.1.12 immediately inform the Controller, if in the opinion of the Processor, an instruction from the Controller infringes Data Protection Legislation.
- 3.2 The Processor will promptly comply with any request by or instruction from the Controller to process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.
- 3.3 The Processor will keep all Personal Data confidential and not disclose such data to third parties unless specifically authorised in writing by the Controller or as required by law. If the Processor is required by law, court, regulator or supervisory authority to process or disclose any Personal Data, the Processor will first inform the Controller of this and allow the Controller to object or challenge the requirement, unless the law prohibits the Processor from informing the Controller.

#### **4 SUBCONTRACTORS**

- 4.1 The Processor may only authorise a third party ("subcontractor") to process the Personal Data if:
- 4.1.1 the Processor has obtained the prior written consent from the Controller for each appointment of a subcontractor (or the subcontractor's name is set out in Schedule 1); and
  - 4.1.2 the Processor has carried out appropriate due diligence on any subcontractor to ensure that the subcontractor can satisfy its contractual obligations; and

- 4.1.3 the Processor and the subcontractor enter into a written contract containing terms the same as those set out in this Agreement, in particular, in relation to data security measures; and
- 4.1.4 the Processor maintains control over all Personal Data it shares with the subcontractor; and
- 4.1.5 the Processor ensures that the subcontractor does not process the Personal Data except on instructions from the Data Controller (unless required to do so by UK Law and/or Union or Member State law); and
- 4.1.6 the contract between the Processor and the subcontractor terminates automatically on termination of this Agreement.

4.2 The Processor shall be fully liable for the actions and inactions of the subcontractor and shall be responsible for the subcontractor's performance of obligations.

## **5. SECURITY**

5.1 The Processor shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate:

- 5.1.1 the pseudonymisation and encryption of Personal Data;
- 5.1.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- 5.1.3 the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- 5.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

5.2 In assessing the appropriate level of security, the Processor shall take account in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

## **6. RESPONSES TO DATA SUBJECTS**

6.1 The Processor will put in place such technical and organisational measures as may be appropriate to enable the Controller to comply with the rights of Data Subjects under Data Protection Legislation, including the right of access, the right to rectification, the right to erasure, the right to restriction of processing, the right to data portability, the right to object to processing and the right to object to automated individual decision making.

6.2 If the Processor receives any complaint or other communication relating to the processing of the Personal Data or a Subject Access Request from a Data Subject, it must notify the Controller as soon as possible after it receives it and in any event within 3 working days and will provide the Controller with all reasonable assistance in helping the Controller to reply

to such communications.

6.3 The Processor will provide to the Controller such information as the Controller may reasonably require in order for the Controller to comply with the rights of Data Subjects under Data Protection Legislation. The Processor may not charge an additional amount for fulfilling its obligations under this clause 6.

6.4 The Processor will provide all appropriate assistance to the Controller to enable it to comply with any information or assessment notices served on the Controller by any supervisory authority under the Data Protection Legislation.

6.5 The Processor shall not disclose Personal Data to any third party other than at the Controller's written request or as set out in this agreement or as required by law.

## **7. PERSONAL DATA BREACH**

7.1 If any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable ("Personal Data Loss"), the Processor will notify the Controller without undue delay (and in any event within 24 hours) after learning of such Personal Data Loss and the Processor shall to the extent possible restore any such data at its own expense.

7.2 If the Processor becomes aware of any unauthorised or unlawful processing of the Personal Data or any Personal Data Breach, it will notify the Controller without undue delay (and in any event within 24 hours) including all relevant information such as:

(a) a description of the nature of the Personal Data Breach, the unauthorised or unlawful processing and/or the Personal Data Loss, including the categories and approximate number of both Data Subjects and Personal Data records concerned;

(b) the likely consequences; and

(c) description of the measures taken, or proposed to be taken, including measures to mitigate the impact.

7.3 The parties will co-ordinate and co-operate with each other to investigate any matters arising as contemplated by this clause.

7.4 The Processor shall take all reasonable steps to mitigate the effects and reduce the impact of any Personal Data Breach or unlawful Personal Data processing.

7.5 The Processor agrees that it shall not (and the Controller is solely responsible to):

(a) provide notice of the Personal Data Breach to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or any other third party, except when the Processor (as opposed to the Controller) is required by law or regulation to provide such notice; and

(b) offer any type of remedy to affected Data Subjects.

7.6 The Processor will cover all reasonable expenses associated with the performance of its obligations under this clause 7.

## **8. CROSS-BORDER TRANSFERS OF PERSONAL DATA**

8.1 The Processor (or any subcontractor of the Processor) shall not transfer or otherwise process Personal Data outside the

UK [or the European Economic Area (EEA)] without obtaining the Controller's prior written consent (except where the Processor is required to transfer such data by UK law [and/or Union or Member State law], in which case the Processor shall inform the Controller of such legal requirement before processing takes place, unless any law prohibits such disclosure on important grounds of public interest).

8.2 If the Controller consents to the transfer or other processing of the Personal Data outside of the UK [and/or the EEA (as the case may be)] and no appropriate safeguards exist (such as an adequacy decision), the Processor and the Controller will each execute the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Schedule to Commission Decision 2010/87/EU ("SCCs") (or the UK approved versions of the same as the case may be).

8.1 If the Processor is based outside of the UK [or the EEA] and is not established within a country for which there are relevant regulator approved safeguards in place such as an adequacy decision, the Processor shall, prior to any Personal Data relating to data subjects within the UK [or the EEA] being transferred to it, execute the European Commission's Standard Contractual Clauses (controller-to-processor transfers), as set out in the Schedule to Commission Decision 2010/87/EU ("SCCs") (or the UK approved versions of the same as the case may be).

8.2 if the Processor appoints subcontractors that are based outside of the UK [or the EEA], the Processor shall, prior to any Personal Data being transferred to such countries, (i) ensure that such subcontractor executes the SCCs and (ii) send a copy of such executed SCCs to the Controller (or the UK approved versions of the same as the case may be).

## **9. TERM AND TERMINATION**

9.1 This Agreement will continue for so long as the Processor processes any Personal Data related to the Services Agreement (**Term**).

9.2 If the Processor breaches this Agreement, such breach shall constitute a material breach of the Services Agreement and the Controller may terminate the Services Agreement immediately on written notice to the Processor without further liability or obligation for the Controller.

## **10. DATA RETURN AND DESTRUCTION**

10.1 The Processor will, on the request of the Controller, provide the Controller with a copy of or access to the Personal Data in its possession or control in the format and on the media reasonably specified by the Controller.

10.2 On termination or expiry of the Services Agreement (membership), the Processor will as agreed as part of your membership, keep all data processed through Fortuna in an anonymised format for PTUK research purposes only. If the Controller wants specific Data to be deleted, destroyed, returned or retained they will notify the processor accordingly.

10.3 If the Processor is required by any law, regulation, or government or regulatory body to retain any documents or materials, the Processor will inform the Controller in writing of such requirement, providing details of the legal basis for retention and setting out the timings for deletion when such retention period ends.

10.4 If the Controller requires the Processor to delete or destroy certain documents or materials or anything else containing

Personal Data, the Processor shall certify in writing that it has so deleted or destroyed the Personal Data within 3 days of doing so.

## **11. RECORDS**

The Processor will keep detailed, accurate and up-to-date written records regarding any processing of Personal Data it carries out for the Controller, using the schedule set out in schedule 3 or in such form as the Controller may require from time to time (**Records**) and shall send the Records to the Controller on a monthly basis (or such other period as required by the Controller).

11.2 The Processor will ensure that the Records are sufficiently detailed to enable the Controller to confirm the Processor's compliance with its obligations under this Agreement and Data Protection Legislation.

11.3 The Controller and the Processor shall review the information listed in the Schedules to this Agreement at least once a year to confirm their current accuracy and update them when required to reflect current practices.

## **12. AUDIT**

12.1 The Controller (and any third-party representatives) may audit the Processor's compliance with its obligations under this Agreement and the Processor will give the Controller (and its third-party representatives) all necessary assistance and co-operation to conduct such audits.

12.2 If a Personal Data Breach occurs, or the Processor becomes aware of a breach of any of its obligations under this Agreement or any Data Protection Legislation, or if the Controller so requires it, the Processor will:

- (a) conduct its own investigation to confirm the cause of such Personal Data Breach or breach of obligations;
- (b) provide to the Controller a written report on the investigation including any proposals to remedy any problems identified by the investigation; and
- (c) remedy the problems identified within 7 days of the date of the written report.

12.3 On the Controller's written request, the Processor will audit a subcontractor's compliance with its obligations regarding the Controller's Personal Data and provide the Controller with the audit results.

12.4 The Processor will carry out an annual security audit (or at such other periods required by the Controller) identifying any areas of deficiency (when taking into account the scope and nature of the processing of Personal Data and the best practice technologies available at such time) and will provide the written report to the Controller.

## **13. WARRANTIES**

The Processor warrants and represents that:

- (a) its employees, subcontractors, agents and any other person or persons processing Personal Data on its behalf are reliable and trustworthy and have received the required training on the Data Protection Legislation;
- (b) it and anyone operating on its behalf will process the Personal Data in compliance with the Data Protection Legislation and;

(c) it has no reason to believe that the Data Protection Legislation prevents it from providing any of the Services Agreement's contracted services.

#### **14. INDEMNIFICATION**

14.1 The Processor agrees to indemnify and keep indemnified the Controller against all costs, claims, damages, expenses or any other liability (including reasonable professional fees) incurred by the Controller (or for which the Controller may become liable) due to any failure by the Processor or its employees, subcontractors or agents to comply with any of its obligations under this Agreement or the Data Protection Legislation.

14.2 Any limitation of liability set out in the Services Agreement will not apply to this Agreement's indemnity.

#### **15. NOTICE**

15.1 Any notice or other communication given to a party under or in connection with this Agreement must be in writing and delivered to:

**Play Therapy (UK) – The United Kingdom Society for Play and Creative Arts Therapies Limited (PTUK)** at email [dataprotection@ptukorg.com](mailto:dataprotection@ptukorg.com)

15.2 Clause 15.1 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

#### **16. GOVERNING LAW**

16.1 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), shall be governed by, and construed in accordance with the law of England and Wales.

16.2 Each party irrevocably agrees that the courts of England and Wales shall have non-exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this agreement or its subject matter or formation (including non-contractual disputes or claims).

This agreement has been entered into on the date stated at the beginning of your membership.

**SCHEDULE 1**

**PERSONAL DATA PROCESSING PURPOSES AND DETAILS**

Subject matter of processing:

**Client data for the purposes of child play therapy and evaluation.**

Duration of Processing:

**THE DURATION OF THE DATA PROCESSING UNTIL THE MEMBERSHIP IS CANCELLED**

Nature and Purpose of Processing:

**To provide CRM services for Play Therapy during the training of therapists and thereafter as members of PTUK**

Data Subject Categories:

**CLIENTS AND FAMILY CONNECTIONS, THERAPISTS NOTES**

Personal Data Types:

**CLIENT Data: Name, Address, Tel, email, parents details, sibling details, medical information, dates and times of appointments**

**Approved Subcontractors:**

<b>NAME OF SUBCONTRACTOR</b>	<b>LOCATION</b>	<b>CONTACT DETAILS FOR PERSON RESPONSIBLE FOR DATA PROTECTION</b>
Fortuna (the system) is hosted by ZoHo, our ZoHo IT specialist will enable new memberships and provide CRM site assistance and issue resolving	Uckfield	Contact to be made via PTUK: <a href="mailto:dataprotection@ptukorg.com">dataprotection@ptukorg.com</a>

## SCHEDULE 2

### SECURITY MEASURES

The technical and organizational data security measures to be taken by the Processor include:

**Keeping all passwords secure at all times to prevent disclosure to any third parties.**

**Retaining all personal data on existing systems used by the Controller and not transferring, downloading, printing, migrating such data to any other systems or otherwise dealing with such data in any other way than using it within the confines of those systems.**

**Ensuring that all software and/or hardware used by the Processor is secure and virus free that the use of such software and/or hardware will do nothing to harm the systems used by the Controller.**

- Fortuna is a HTTP protected Web site.
- Fortuna is encrypted – see below.  
([https://help.zoho.com/portal/en/kb/creator/developer-guide/applications/articles/encryption-in-zoho-creator#Encryption\\_at\\_Rest](https://help.zoho.com/portal/en/kb/creator/developer-guide/applications/articles/encryption-in-zoho-creator#Encryption_at_Rest))

**Not allowing any persons other than PTUK to process the Personal Data**

**NOTE THE FOLLOWING RESOURCES MAY HELP IN TERMS OF THE TYPES OF SECURITY YOUR SUPPLIER SHOULD BE CONSIDERING:**

[https://ico.org.uk/media/for-organisations/documents/1575/it\\_security\\_practical\\_guide.pdf](https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf)

<https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/>

**SCHEDULE 3**

**RECORDS OF PROCESSING**

	<b>Access, control and security</b>	<b>Approved subcontractors</b>	<b>Processing Purposes</b>	<b>Categories of processing</b>	<b>Transfers outside of EEA and safeguards</b>	<b>Security measures</b>
Ongoing	Limited access to Fortuna, Data Controller + IT services (when required) and names staff from PTUK. All other staff see anonymised data only	Relativity – Local ZoHo IT specialist	Controller loads information from therapy sessions for use as a CRM system. This information once anonymised is then used for research purposes.	<b>Name, Address, Tel, email, parent’s details, sibling details, medical information, dates and times of appointments</b>	Data is stored in the EEA but can be accessed globally	Individual sign on, Encryption, password protection,

**[NOTE: if you are unsure about what security measures you have (or should have) in place, see:**

<https://www.cyberessentials.ncsc.gov.uk/advice/> ]