

# Tudor Business Services Ltd GDPR Addendum (Addendum)

## 1. Definitions

1. In this Addendum the following definitions shall apply:

<b>Controller</b>	Has the meaning given in applicable Data Protection Laws from time to time;
<b>Data Protection Laws</b>	means, as binding on either party or the Services: <ul style="list-style-type: none"><li>a. The Directive 95/46/EC (Data Protection Directive) and/or Data Protection Act 1998 or the GDPR;</li><li>b. Any laws which implement any such laws; and</li><li>c. Any laws that replace, extend, re-enact, consolidate or amend any of the foregoing;</li></ul>
<b>Data Subject</b>	Has the meaning given in applicable Data Protection Laws from time to time;
<b>GDPR</b>	means the General Data Protection Regulation (EU) 2016/679;
<b>International Organisation</b>	has the meaning in the GDPR;
<b>Personal Data</b>	has the meaning given in applicable Data Protection Laws from time to time;
<b>Personal Data Breach</b>	has the meaning given in the GDPR;
<b>Processing</b>	has the meaning given in applicable Data Protection Laws from time to time (and related expressions, including <b>process, processed, processing, and processes</b> shall be construed accordingly);
<b>Processor</b>	has the meaning given in applicable Data Protection Laws from time to time;
<b>Sub-Processor</b>	means any agent, subcontractor or third party (excluding its employees) engaged by the Supplier for carrying out any processing activities on behalf of the Customer in respect of the Protected Data.

## 2. Customer's Compliance with Data Protection Laws

- a. The parties agree that you (referred to in this Addendum as the "**Customer**"), are a Controller and that we (referred to in this Addendum as the "**Supplier**") are a Processor for the purposes of processing Protected Data pursuant to the Agreement.
- b. The Customer shall at all times comply with all Data Protection Laws in connection with the processing of Protected Data.
- c. The customer shall ensure all instructions given by it to the supplier in respect of Protected Data (including the terms of the Agreement) shall be given in a clear manner without delay or conditions and shall at all times be in accordance with Data Protection Laws.

### **3. Supplier's Compliance with Data Protection Laws**

The Supplier shall process Protected Data in compliance with the obligations placed on it under Data Protection Laws and Section 1 of the Schedule to this Addendum and the Agreement.

### **4. Indemnity**

The Customer shall indemnify and keep indemnified the Supplier against all losses, claims, damages, liabilities, fines, sanctions, interest, penalties, costs, charges, expenses, compensation paid to Data subjects, demands and legal and other professional costs (calculated on a full indemnity basis and in each case whether or not arising from any investigation by, or imposed by, a supervisory authority) arising out of or in connection with any breach by the Customer of its obligations under this Addendum.

### **5. Instructions**

- a) The Supplier shall only process (and shall ensure Supplier Personnel only process) the Protected Data in accordance with section 2 of the Schedule to this Addendum and the Agreement (and not otherwise unless alternative processing instructions are agreed between the parties in writing) except where otherwise required by applicable law (and shall inform the Customer of the legal requirement before processing, unless applicable law prevents it doing so on important grounds of public interest)
- b) Without prejudice to paragraph 2 of this Addendum, if the Supplier reasonably believes that any instruction received by it from the Customer may infringe the Data Protection Laws it shall promptly inform the Customer and be entitled to cease to provide the relevant services without liability under the Agreement until the parties have agreed appropriate amended instructions which are not infringing.

### **6. Security**

Taking into account the state technical development and the nature of processing, the Supplier shall implement and maintain such technical and organisational measures as may reasonably be required to protect the Protected Data against accidental, unauthorised or lawful destruction, loss, alteration, disclosure or access.

### **7. Sub-processing and Personnel.**

The supplier shall:

- a) Not permit and processing of Protected Data by any agent, subcontractor or other third party (except its or its Sub-Processors own employees in the course of their employment that are subject to an enforceable obligation of confidence with regards to the Protected Data) without the prior written authorisation of the Customer;
- b) Prior to the relevant Sub-Processor carrying out any processing activities in respect of the Protected Data, appoint each Sub-Processor under a written contract containing materially the same obligations as under this Addendum that is enforceable by the Supplier and ensure each such Sub-Processor complies with all such obligations;

- c) Remain fully liable to the Customer under the Agreement for all the acts and omissions of each Sub-Processor as if they were its own; and
- d) Ensure that all persons authorised by the Supplier or any Sub-Processor to process Protected Data are subject to a binding written contractual obligation to keep the Protected Data Confidential.

## **8. Assistance**

- a) The Supplier shall (At the Customer's cost) assist the Customer in ensuring compliance with the Customer's obligations pursuant to Articles 32 to 36 of the GDPR (and any similar obligations under applicable Data Protection Laws) taking into account the nature of the processing and information available to the Supplier.
- b) The Supplier shall (at the Customer's cost) taking into account the nature of the processing, assist the Customer (by appropriate technical and organisational measures), insofar as this is possible, for the fulfilment of the Customer's obligations to respond to the requests for exercising the Data Subjects' rights under Chapter III of the GDPR (and any similar obligations under applicable Data Protection Laws) in respect of any Protected Data.

## **9. International Transfers**

The supplier shall not process and/or transfer, or otherwise directly or indirectly disclose, any Protected Data in or to countries outside the United Kingdom or to any International Organisation without the prior written consent of the Customer.

## **10. Audits & Processing**

The Supplier shall, in accordance with Data Protection Laws, make available to the Customer such information that is in its possession or control as is necessary to demonstrate the Supplier's compliance with the obligations placed on it under this Addendum and to demonstrate compliance with the obligations on each party imposed by Article 28 of the GDPR (and under any equivalent Data Protection Laws (and under any equivalent Data Protection Laws equivalent to that Article 28), and allow for and contribute to audits, including inspections, by the Customer (or another auditor mandated by the Customer) for this purpose (subject to a maximum of one audit request in any 12 month period under this paragraph 10).

## **11. Deletion/Return & Survival**

On the end of the provision of the Services relating to the processing of Protected Data, at the Customer's cost and the Customer's option, the Supplier shall either return all of the Protected Data to the Customer or securely dispose of the Protected Data (and thereafter promptly delete all existing copies of it) except to the extent that any applicable law requires the Supplier to store such Protected Data. The Addendum shall survive termination or expiry of the Agreement for 18 months following the earlier of the termination or expiry of the Agreement.

# Schedule

## Section 1

### Data Processing Details

The Processing of the Protected Data by the Supplier under the Agreement shall be for the subject-matter, duration, nature and purposes and involve the types of Personal Data and categories of Data Subjects set out below.

1. **Subject-matter of Processing:**

The Supplier's provision of Services to the Customer under the Agreement.

2. **Duration of the Processing:**

The term set out in the Agreement plus the period from the expiry of the term until deletion of all Customer data by the Supplier in accordance with the Agreement.

3. **Nature and Purpose of the Processing**

The Supplier will process Customer Personal Data for the purposes of providing the Services to the Customer in accordance with the Agreement.

4. **Type of Personal Data:**

Personal Data relating to individuals provided to the Supplier in order for the Supplier to provide Services, by (or at the direction of) the Customer or by the Customer end users including but not limited to name, address, telephone number, email address, identification number, location data or online identifier.

5. **Categories of Data Subjects:**

Data Subjects include the individuals about whom the data is provided to the Supplier for the purpose of the provision of the Services by (or at the direction of) the Customer or by the Customer end users.

## Section 2

### Minimum Technical & Organisational Security Measures

The Supplier shall implement and maintain the following technical and organisational security measures to protect the Protected Data:

**Infrastructure.** The supplier stores all production data in physically secure locations within the United Kingdom and European Union.

**Environmental Redundancy.** All environmental equipment and facilities have preventative maintenance procedures.

**Power.** Mains power protection is provided during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power and controlled, safe shutdown of systems.

**Server Operating Systems.** All IT infrastructure utilises industry standard enterprise level Operating Systems which are regularly patched in accordance with the software vendor's recommendation. All systems are protected with anti-virus, anti –malware and anti-ransomware software, as appropriate.

**Business Continuity.** The Supplier maintains a cloud-based backup and replication systems and regularly plans and tests its business continuity/disaster recovery procedures.

**Data Transmission.** To prevent data from being read, copied, altered or removed without authorisation the Supplier encrypts and/or password protects all transmissions containing Personal Data.

**Encryption Technologies.** The Supplier uses AES and/or HTTPS encryption (also referred to as a SSL or TLS connection) as appropriate.