

Tax Computer Systems Limited Data Processing Addendum

This Data Processing Addendum (the "**Addendum**") amends the terms of the Tax Computer Systems Limited ("TCSL") Master Services Agreement or Licence Agreement or Services Agreement, as applicable, (the "**Agreement**") between TCSL and you.

With effect from the 25th May 2018, this Addendum shall apply to personal data that TCSL ("**TCSL**," "**we**," "**us**," or "**our**") processes in the course of providing you the Software and/or Hosted Services (collectively, "**Software**") under the Agreement.

The scope and duration, as well as the extent and nature of the collection, processing and use of personal data under this Addendum shall be as defined in the Agreement. The term of this Addendum corresponds to the duration of the Agreement. Please download and sign a copy of this Addendum and send the same through to us to acknowledge the changes made to the Agreement by this Addendum.

1. DEFINITIONS:

1.1 The terms below shall have the following meanings;

"**You**" or "**your**" means the Customer;

"**Customer Personal Data**" means the personal data processed by TCSL on your behalf in the course of providing Products to you, other than TCSL Business Contact Data.

"**TCSL Business Contact Data**" means personal data processed by TCSL for billing purposes, to send information about our new products and services, to improve our products and services and provide support, to comply with law (including law enforcement requests) and to ensure security of our services and to prevent fraud or mitigate risk;

"**Data Protection Legislation**" Means (i) the GDPR, the Law Enforcement Directive and any applicable national implementing Laws as amended from time to time (iii) the Data Protection Act 2018 to the extent that it relates to personal data and privacy (iii) all applicable law about the processing of personal data and privacy (including but not limited to the Directive on Privacy and Electronic Communications (as amended) and any e-privacy Regulation in force from time to time);

"**data processor**", "**data subject**", "**personal data**", "**processing**" and "**appropriate technical and organisational measures**" shall be interpreted in accordance with applicable Data Protection Legislation; and

"**Software**", "**Hosted Services**" and "**Authorised Users**" shall have the meaning set forth in the Agreement (as applicable).

2. DATA PROTECTION

2.1 The provisions of this Section 2 shall apply where Data Protection Legislation apply to your processing of Customer Personal Data and where we process that Customer Data in the course of providing you the Software. We are the data processor in relation to Customer Personal Data.

2.2 The subject-matter of the data processing is providing the Software, Support and Professional Services (as defined in the Agreement) and the processing will be carried

out until we cease to provide any Software, Support and Professional Services to you. Annex 1 of this Addendum sets out the nature and purpose of the processing, the types of Customer Personal Data we process and the data subjects whose Customer Personal Data is processed.

- 2.3 When we process Customer Personal Data in the course of providing Software to you, we will:
- 2.3.1 process the Customer Personal Data only in accordance with documented instructions from you (as set forth in this Addendum or the Agreement or as directed by you through the Service). If applicable law requires us to process the Customer Personal Data for any other purpose, we will inform you of this requirement first, unless such law(s) prohibit this on important grounds of public interest;
 - 2.3.2 notify you promptly if, in our opinion, an instruction for the processing of Customer Personal Data given by you infringes applicable Data Protection Legislation;
 - 2.3.3 assist you, taking into account the nature of the processing:
 - (i) by appropriate technical and organisational measures and where possible, in fulfilling your obligations to respond to requests from data subjects exercising their rights;
 - (ii) in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the General Data Protection Regulation, taking into account the information available to us; and
 - (iii) by making available to you all information reasonably requested by you for the purpose of demonstrating that your obligations relating to the appointment of processors as set out in Article 28 of the General Data Protection Regulation have been met.
 - 2.3.4 implement and maintain appropriate technical and organisational measures to protect the Customer Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure in accordance with Annex 2. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful processing, accidental loss, destruction, damage or theft of Customer Personal Data and appropriate to the nature of the Customer Personal Data which is to be protected. We may amend the technical and organisational measures, provided that the new measures do not fall short of the level of security provided by the specified measures. Substantial changes must be documented;
 - 2.3.5 not give access to or transfer any Customer Personal Data to any third party for such third party's independent use (e.g., not directly related to providing the Software) without your prior written consent. You consent to our appointment of the subprocessors listed at www.taxsystems.com/dpa-subprocessors for the purposes described in this Addendum provided that we take reasonable steps that each of the subprocessors listed complies at all times with the relevant Data Protection Legislation and shall not perform their obligations under this Addendum in such a way as to cause either party

to breach any of its obligations under the Data Protection Legislation. We will notify you in writing of any changes to the list of approved subprocessors, at which point you will have the opportunity to object by terminating the Agreement. When engaging subprocessors in the processing of Customer Personal Data, we are responsible for the conduct and performance of each subprocessor. We will include in our agreement with any such third party subprocessor terms which are at least as favourable to you as those contained herein and as are required by applicable Data Protection Legislation;

- 2.3.6 ensure that our personnel required to access the Customer Personal Data are subject to a binding duty of confidentiality with regard to such Customer Personal Data;
 - 2.3.7 except as set forth in Section 2.3.5 above or in accordance with documented instructions from you (as set forth in this Addendum or the Agreement or as directed by you through the Service), ensure that none of our personnel publish, disclose or divulge any Customer Personal Data to any third party; and
 - 2.3.8 upon expiration or earlier termination of the Agreement, upon your written request, securely destroy or return to you such Customer Personal Data, and destroy existing copies unless applicable laws require storage of such Customer Personal Data.
- 2.4 If we become aware of and confirm any accidental, unauthorised or unlawful destruction, loss, alteration, or disclosure of, or access to your Customer Personal Data that we process in the course of providing the Software (a "**Security Breach**"), we will notify you within forty-eight hours.
- 2.5 All Customer Personal Data processing takes place within the European Economic Area ("**EEA**"). We will not transfer Customer Personal Data outside the European Economic Area without prior notice to you and, where notice is given to you of such transfer, we will:
- (i) provide an adequate level of protection to any Customer Personal Data that is transferred; and
 - (ii) comply with your reasonable instructions notified to us.
- 2.6 Through use of the Software, as further described in the Agreement, you may elect to grant third parties visibility to your data or content (which may include Customer Personal Data). Nothing in this Addendum prohibits (and, for the avoidance of doubt, Sections 2.3.5 and 2.3.7 above do not apply to) TCSL's making visible your data or content (which may include Customer Personal Data) to third parties consistent with this paragraph, as directed by you through the Software.

3. MISCELLANEOUS

- 3.1 Where you use several of our Software modules, you acknowledge that we may combine information from your use of the Software to deliver integrated services across the suite of Software that you have purchased (for example to allow you to search across our Software or to combine notifications from multiple Software). You also acknowledge that we may process information generated by your users for research and analytical purposes, in order to improve, benchmark and develop our Software. We will ensure that the results of this processing do not identify you or any of your

users and that all such processing is subject to appropriate technical and organisational measures.

- 3.2 In the event of any conflict or inconsistency between the provisions of the Agreement and this Addendum, the provisions of this Addendum shall prevail. For avoidance of doubt and to the extent allowed by applicable law, any and all liability under this Addendum will be governed by the relevant provisions of the Agreement, including limitations of liability. Save as specifically modified and amended in this Addendum, all of the terms, provisions and requirements contained in the Agreement shall remain in full force and effect and govern this Addendum. Except as otherwise expressly provided herein, no supplement, modification, or amendment of this Addendum will be binding, unless executed in writing by a duly authorised representative of each party to this Addendum. If any provision of the Addendum is held illegal or unenforceable in a judicial proceeding, such provision shall be severed and shall be inoperative, and the remainder of this Addendum shall remain operative and binding on the parties.
- 3.3 This Addendum and any dispute or claim (including non-contractual disputes or claims) that arises out of, or in connection herewith shall be governed by and construed in accordance with the laws of England and Wales. Any dispute, controversy, proceedings or claim between the parties relating to this Addendum (including any non-contractual matters and obligations arising therefrom or associated therewith) shall fall within the jurisdiction of the courts of England and Wales.

Please sign and return the enclosed copy of this Addendum to acknowledge the supplementation of these terms to the Agreement.

Customer:

Name:

Title:

Signature:

Date:

Data Protection Officer (where applicable):

Contact details:

TCSL

Name: Kevin Goggin

Title: Director

Signature: 04CCF2EE32804B7...

Date: January 9, 2019 | 02:36 PST

Data Protection Point of Contact:

Contact details: dpo@taxsystems.com

Annex 1

Data subjects

The End Users of our Products, in addition to individuals whose personal data is supplied by the End Users of the Software.

Categories of data

Personal Data

The personal data we process include the following categories:

- Direct identifying information (e.g., name, email address, telephone).
- Indirect identifying information (e.g., job title, gender, national insurance number).
- Device identification data and traffic data (e.g., IP addresses, MAC addresses, web logs).
- Any personal data supplied by users of the Software.

Special categories of data

Tax Systems does not knowingly collect (and Customer or End Users shall not submit or upload) any special categories of data (as defined under the Data Protection Legislation).

Purposes of processing

The personal data is processed for the purposes of providing the Software in accordance with the Agreement.

Annex 2

Security Measures

Organisation of Information Security

- Clear and explicitly assigned management commitment to information security is allocated throughout the organisation, with specific allocation of information security responsibilities outlined in the policies and procedures in use within the company.

Asset Management

- Tax Systems understands the importance of asset ownership and all assets are clearly identified and registered.
- Staff are also informed and reminded as to the acceptable use of assets with regular awareness training.

Human Resource Security

- Employees are screened prior to employment to ensure suitability for their role using the following mechanisms:
 - Education and employment references
 - Qualification checks
 - DBS background checks
- Continuous awareness surrounding Information Security is given with specific sessions for key staff.
- When a member of staff leaves, no matter what the circumstance, a leaver process is followed to prevent accidental or deliberate account misuse or loss of information assets.

Communications and Operations Management

- The correct and secure operation of Tax Systems information processing facilities is ensured by strict change management/change control process.
- Separate live, test and development environments are utilised to reduce the risks of unauthorised access or changes.
- Enterprise level anti-virus, firewalls, intrusion prevention and mobile device management are in place to protect the Tax Systems environment.
- These systems are centrally managed and automatically updated in line with their vendor's recommendations.

Access Control

- A policy of least privilege access and need to know is applied to Tax Systems computer systems and data.
- This policy ensures Tax Systems staff only have the minimum access required to perform their jobs.
- Any privileged accounts are rigorously checked both prior to granting access, during use and on termination of permissions.
- All users come under multiple levels of policy regarding accounts and device usage.
- Any sensitive systems are housed in dedicated secure environments.
- Measures must be taken to prevent unauthorised physical access to premises and facilities holding personal data.
- All remote access must be strictly controlled and properly secured.

Information Systems Acquisition, Development & Maintenance

- Requirements for security controls are addressed prior to any new system or existing system enhancement.
- A multi-level change control system exists to prevent errors occurring either accidentally or maliciously with data validation in place to detect errors.
- Where cryptographic applications are utilised, an appropriate key management system is in place.
- User access to software, test data and source code is restricted and monitored.
- Industry class software is deployed to control external ports on laptops to help prevent data leakage.

Information Security Incident Management

- Security Incident Management processes are aligned with industry best practice.
- Any information security incidents are followed by a full management review and root cause analysis.
- Any necessary post incident investigation will be carried out by suitably trained and experienced staff.

Business Continuity Management

- Appropriate Business Continuity Management processes and documentation are in place, to minimise the impact to services in the event of a disruption.
- A program of testing ensures the suitability of these plans and is reviewed annually.

Compliance

- Tax Systems complies with all relevant requirements and these are tested and/or audited on a regular basis.