THE PC SUPPORT GROUP

THE PC SUPPORT GROUP DATA PROCESSING ADDENDUM

1st Edition February 2022

Data Processing Confirmation

This **Data Processing Addendum** (or '**DPA**') comprises the **Data Processing Confirmation** and **Data Processing Terms** and is entered into by the Client or You ('**Data Controller**'); and The PC Support Group Limited incorporated in England and Wales under company number 02198426 ('**PCSG** or **Data Processor**') pursuant to the **Data Processing Terms** (each a '**Party**' and together the '**Parties**') at Appendix 1.

The **Standard Contractual Clauses** are incorporated herein by reference and shall prevail to the extent that they conflict with the **Data Processing Terms**.

All defined terms are as defined in Appendix 1 below unless otherwise stated in here. The governing law and jurisdiction set out in the **PCSG Terms and Conditions of Business** shall apply to this **DPA**.

1. PARTICULARS

Effective Date	This DPA shall commence on the date of the PCSG Purchase Order.
Data Processor's business or organization type	We are an IT, digital, technology and telecoms organisation which supports businesses with their business automation, data security and information management
Term	The Data Processor will only Process Personal Data for the duration of the DPA which shall start on the PCSG Purchase Order and shall terminate upon termination or expiry of the Services.
Sub-Data Processors	This list is maintained at https://pcsupportgroup.com/sub-processor-list/

2. OVERVIEW OF DATA PROCESSING ACTIVITIES

Categories of Data Subjects: The Personal Data transferred includes but is not limited to the following categories of current, past and prospective Data Subjects. Where any of the following is itself a business or organization, it includes their personnel as applicable to the Processing:
Categories of Personal Data: Due to the nature of PCSG's business, PCSG may process Personal Data that includes but is not limited to the following categories of data: **General:** Personal details, including any information that identifies the data subject and their personal characteristics, including: name, address contact details, age, date of birth, sex, and physical description. Personal details issued as an identifier by a public authority, including passport details, national insurance numbers, identity card numbers, driving licence details. Family, lifestyle and social circumstances, including any information relating to the family of the data subject and the data subject's lifestyle and social circumstances, including current marriage and partnerships, marital history, details of family and other household members, habits, housing, travel details, leisure activities, and membership of charitable or voluntary organisations. Education and training details, including information which relates to the education and any professional training of the data subject, including academic records, qualifications, skills, training records, professional expertise, student and pupil records. Employment details, including information relating to the employment of the data subject, including employment and career history, recruitment and termination details, attendance records, health and safety records, performance appraisals, training records, and security records. Financial details, including information relating to the financial affairs of the data subject, including income, salary, assets and investments, payments, creditworthiness, loans, benefits, grants, insurance details, and pension information. Goods or services provided and related information, including details of the goods or services supplied, licences issued, and contracts. Personal data relating to criminal convictions and offences Other (please provide details of other data subjects): **Special category data:**

Personal Data which reveals, or which concerns:

racial or ethnic origin

political opinions

religious or philosophical beliefs

trade union membership

genetic data

biometric data (if used to identify a natural person)

health

sex life or sexual orientation

criminal convictions and offences

Processing Operations:
The Personal Data transferred will be subject to the following basic Processing Operations:
Receiving data, including collection, accessing, retrieval, recording, and data entry

Holding data, including storage, organisation and structuring

Using data, including analysing, consultation, testing, automated decision making and profiling

Updating data, including correcting, adaptation, alteration, alignment and combination

Protecting data, including restricting, encrypting, and security testing

Sharing data, including disclosure, dissemination, allowing access or otherwise making available

Returning data to the Data Controller or Data Subject

Erasing data, including destruction and deletion

For the following purposes:
IT, digital, technology or telecom services, including provision of technology products or services, telecoms and network services, digital services, hosting, cloud and support services or software licensing; including passwords.

Technical and Organizational Security Measures:
The following checklist and supplementary details set out the description of the Technical and Organisational Security Measures implemented by the Data Processor in accordance with Standard Contractual Clauses 4(d) and 5(c):

We use firewalls to protect our internet connection;
We choose the most appropriate secure settings for our devices and software;
We control who has access to your data and services;
We do this by insisting passwords are compliant with our complex password policy and by issuing multifactor authentication wherever possible;
We protect ourselves from viruses and other malware;
We keep our software and devices up-to-date;
We regularly backup our dataoffsite and in a secure manner.

Data Processing Addendum (DPA)
Appendix 1 Data Processing Terms

Definitions	**Binding Corporate Rules**: shall have the meaning set out in the applicable Privacy Laws. **Control:** means direct or indirect ownership or control of more than 50% of the voting interests of a Party. **Data Breach**: refers to any accidental or unlawful destruction, loss, alteration or unauthorized disclosure or access to any Personal Data. **Data Controller:** shall have the meaning set out in the applicable Privacy Laws as the natural or legal person which decides the purposes and means of Processing data. In this DPA, this is You the Client. **Data Processor:** shall have the meaning set out in the applicable Privacy Laws as the natural or legal person which is responsible for Processing the Personal Data on behalf of the Data Controller. The Data Processor agrees to receive the Personal Data from the Data Controller for Processing on the Data Controller's behalf in accordance with its instructions and the terms herein (and the duly incorporated SCCs where such Processing is subject to a third country's system ensuring adequate protection within the meaning of Article 25 (1) of the GDPR). In this DPA, this is PCSG. **Data Subject:** shall have the meaning set out in the applicable Privacy Law as the individual or household to whom the Personal Data relates. **Data Processing Addendum** or **DPA:** means this document. **DSAR:** refers to a data subject access request which is the right of access as further described in Article 15 of the GDPR. **PCSG Terms and Conditions of Business:** means PCSG IT Terms and Conditions of Engagement, PCSG Terms & Conditions for the Provision of Equipment and/or Mobile Network Services and PCSG Terms & Conditions for the Provision of Equipment, Conference Calling Services, Consultancy Services, Fixed Network Services, Hosting Services, Maintenance Services, and/or WiFi Services. **PCSG Purchase Order:** means the purchase order form or other document issued by PCSG to the Client that sets out the goods and/or services that PCSG supplies to the Client. **Services:** means the services offered to the Clients by PCSG as specified in the Purchase Order. **Standard Contractual Clauses** or **SCCs**: means the EU model clauses for Personal Data transfer from Data Controllers to Data Processors c2010-593 - Decision 2010/87EU **Sub-Data Processor**: means any person or entity engaged by the Data Processor who agrees to receive the Personal Data from the Data Processor or from any other Sub-Data Processor of the Data Processor in order for it to be Processed on behalf of the Data Controller in accordance with its instructions, the terms of the SCCs and the terms of any sub-contract who are referred to in the Data Processing Confirmation. **Supervisory Authority**: an independent national data protection authority such as the ICO in the UK. **Technical and Organizational Security Measures**: means those measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular, where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing.
Introduction	The Data Processor has agreed to provide the Services to the Data Controller in accordance with the Agreement. In providing the Services, the Data Processor shall Process the Personal Data referred to in the **Data Processing Confirmation** on behalf of the Data Controller. The Data Processor will Process and protect such Personal Data in accordance with the terms of this DPA.
Scope	Data Processor shall Process Personal Data only to the extent necessary to provide the Services in accordance with both the Agreement and the Data Controller's instructions documented in the Agreement and this DPA. The scope of the Processing is set out in the Data Processing Confirmation.
Your obligations as Data Controller	The Data Controller represents and warrants that it shall comply with the Agreement, this DPA and all Applicable Data Protection Law. The Data Controller represents and warrants that it has obtained any and all necessary permissions and authorizations necessary to permit the Data Processor and Sub-Data Processors, to execute their rights or perform their obligations under this DPA. The Data Controller is responsible for compliance with all Applicable Data Protection Law, including requirements with regards to the transfer of Personal Data under this DPA and the Agreement. The Data Controller shall implement appropriate Technical and Organizational Security Measures to protect Personal Data, 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.

	The Data Controller shall take steps to ensure that any natural person acting under the authority of the Data Controller who has access to Personal Data only Processes the Personal Data on the documented instructions of the Data Controller. The Data Controller may require correction, deletion, blocking and/or making available the Personal Data during or after termination of the Agreement. The Data Processor will Process the request to the extent it is lawful and will reasonably fulfil such request in accordance with its standard operational procedures to the extent possible. The Data Controller acknowledges and agrees that some instructions from the Data Controller, including destruction or return of data, assisting with audits, inspections or data protection impact assessments by the Data Processor, may result in additional reasonable fees. In such case, the Data Processor will notify the Data Controller of its fees for providing such assistance in advance, unless otherwise agreed.
Our obligations as Data Processor	The Data Processor may Process Personal Data only within the scope of this DPA. The Data Processor confirms that it shall Process Personal Data on behalf of the Data Controller and shall take steps to ensure that any natural person acting under the authority of the Data Processor who has access to Personal Data shall only Process the Personal Data on the documented instructions of the Data Controller. The Data Processor shall ensure that all employees, agents, officers and contractors involved in the handling of Personal Data: have received appropriate training on their responsibilities as a Data Processor; and, are bound by the terms of this DPA. The Data Processor shall promptly inform the Data Controller, if in the Data Processor's opinion, any of the instructions regarding the Processing of Personal Data provided by the Data Controller, breach any Applicable Data Protection Law. The Data Processor shall implement appropriate Technical and Organizational Security Measures to protect Personal Data, 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. The Data Processor shall implement appropriate Technical and Organizational Security Measures to ensure a level of security appropriate to the risk as set out in the Data Processing Confirmation. The Data Controller accepts and agrees that the Technical and Organizational Security Measures are subject to development and review and that the Data Processor may use alternative suitable measures to those detailed therein where necessary. The Data Processor shall make available to the Data Controller all information reasonably necessary to demonstrate compliance with its Processing obligations and allow for and contribute to remote audits and inspections. Any audit conducted under this DPA shall consist of examination of the most recent reports, certificates and/or extracts prepared by an independent auditor bound by confidentiality provisions similar to those set out in the Agreement. In the event that provision of the same is not deemed sufficient in the reasonable opinion of the Data Controller, the Data Controller may conduct a more extensive remote audit which will be: (i) at the Data Controller's expense; (ii) limited in scope to matters specific to the Data Controller and agreed in advance; (iii) carried out during UK business hours and upon reasonable notice which shall be not less than 4 weeks unless an identifiable material issue has arisen; and (iv) conducted in a way which does not interfere with the Data Processor's day-to-day business.
Liability	The limitations on liability set out in the PCSG Terms and Conditions of Business apply to all claims made pursuant to any breach of the terms of this DPA by the Data Processor. The Parties agree that the Data Processor shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Sub-Data Processors subject to any limitations on liability set out in the terms of the Agreement. The Parties agree that the Data Controller shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Affiliates as if such acts, omissions or negligence had been committed by the Data Controller itself. The Data Controller shall not be entitled to recover more than once in respect of any one same

	claim.
Notification of a Data Breach	The Data Processor shall notify the Data Controller without undue delay after becoming aware of any Data Breach. Such notification of, or response to, a Data Breach shall not be construed as an acknowledgement by the Data Processor of any fault or liability with respect to the Data Breach. Upon becoming aware of a Data Breach in respect of Personal Data Processed by the Data Processor on behalf of the Data Controller under this DPA, the Data Processor will take all commercially reasonable measures to secure the Personal Data, to limit the effects of any Data Breach, and to assist the Data Controller in meeting the Data Controller's obligations under the Applicable Data Protection Law.
Co-operation (with each other and with Supervisory Authorities), compliance and Response	In the event that the Data Processor receives a DSAR from a Data Subject in relation to Personal Data, the Data Processor will refer the Data Subject to the Data Controller unless otherwise prohibited by law. The Data Controller shall reimburse the Data Processor for all costs incurred resulting from providing reasonable assistance in dealing with a DSAR. In the event that the Data Processor is legally required to respond to the Data Subject, the Data Controller will fully cooperate with the Data Processor as applicable. The Data Processor will notify the Data Controller promptly of any request or complaint regarding the Processing of Personal Data, which adversely impacts the Data Controller, unless such notification is not permitted under applicable law or a relevant court order. The Data Processor may make copies of, and/or retain, Personal Data in compliance with any legal or regulatory requirement including, but not limited to, retention requirements. The Data Processor shall reasonably assist the Data Controller in meeting its obligation to carry out data protection impact assessments, taking into account the nature of Processing and the information available to the Data Processor. The Data Processor shall respond within a reasonable timeframe in respect of any changes that need to be made to the terms of this DPA or to the Technical and Organizational Security Measures to maintain compliance. If the Parties agree that amendments are required, but the Data Processor is unable to (promptly) accommodate the necessary changes, the Data Controller may terminate its' own use of the part or parts of the Services which gives rise to the non-compliance. To the extent that other parts of the Services provided are not affected by such changes, the provision of those Services shall remain unaffected. The Data Controller and the Data Processor and, where applicable, their representatives, shall cooperate, on request, with a Supervisory Authority in the performance of their respective obligations under this DPA.
Sub-Processing & International Transfers	The Data Controller acknowledges and agrees that: Affiliates of the Data Processor may be used as Sub-Data Processors; and, the Data Processor and its Affiliates respectively may engage Sub-Data Processors in connection with the provision of the Services. All Sub-Data Processors who Process Personal Data in the provision of the Services to the Data Controller shall comply with the obligations of the Data Processor set out in this DPA, in particular, in providing at least the same level of protection for the Personal Data and the DSARs as the Data Processor. Where Sub-Data Processors are located outside of the EEA, the Data Processor confirms that such Sub-Data Processors: are located in a third country or territory recognized by the EU Commission to have an adequate level of protection. See list here; or, have entered into the **Standard Contractual Clauses** with the Data Processor; or, have other legally recognized appropriate safeguards in place, such as Binding Corporate Rules. The Data Processor makes available to the Data Controller, the **Sub-Data Processor List** (which includes the identities of Sub-Data Processors and their country of location) which it shall maintain and keep up-to-date. It can be accessed at https://pcsupportgroup.com/sub-processor-list/

	The Data Controller may object to the use of a new or replacement Sub-Data Processor, by notifying the Data Processor. If the Data Controller objects to a new or replacement Sub-Data Processor, and that objection is not unreasonable, the Data Controller may terminate the Agreement with respect to those Services which cannot be provided by the Data Processor without the use of the new or replacement Sub-Data Processor.
Termination	Upon expiry of the Term, the Data Processor shall at the Data Controller's option, delete or return Personal Data to the Data Controller after the end of the provision of the Services in accordance with the Agreement relating to Processing, and delete existing copies unless applicable law or regulations require the retained storage of any part of the Personal Data.