



DATA PROCESSING ADDENDUM

(Revision November 2024)

This Data Processing Addendum, including its Schedules, (“DPA”) forms part of the Master Services Agreement between PCS and Customer for the purchase of Services from PCS (the “Agreement”) to reflect the Parties’ agreement with regard to the Processing of Personal Data.

Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates. For the purposes of this DPA only, and except where indicated otherwise, the term “Customer” shall include Customer and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services to Customer pursuant to the Agreement, PCS and its Affiliates may Process Personal Data on behalf of Customer and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith:

1. DEFINITIONS

“**Authorized Affiliate**” means any of Customer’s Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and PCS, but has not signed its own Order Form with PCS and is not a “Customer” as defined under this DPA.

“**CCPA**” means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., as amended by the California Privacy Rights Act, and its implementing regulations.

“**Controller**” means the entity which determines the purposes and means of the Processing of Personal Data.

“**Data Protection Laws and Regulations**” means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including those of the United Kingdom (UK GDPR), the European Union, the European Economic Area and their member states (GDPR), Australia and its states and United States and its states.

“**Data Subject**” means the identified or identifiable person to whom Personal Data relates.

“**Personal Data**” means 1) any information relating to an identified or identifiable natural person, where such data is Customer Data or 2) Professional Services Data.

“**Processing**” or “**Process**” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“**Processor**” means the entity which Processes Personal Data on behalf of the Controller, including as applicable any “service provider” as that term is defined by the CCPA.

“**Professional Services Data**” means any information relating to an identified or identifiable natural person, where such data is provided by or for Customer to PCS as a Processor in order to perform the Professional Services pursuant to an Agreement.

“**Security and Privacy Documentation**” means the Security and Privacy Documentation applicable to the specific Services purchased by Customer, as updated from time to time, and accessible via PCS’s Trust and Compliance webpage at <https://www.personcentredsoftware.com/legal/trust-and-compliance-documentation>, via login to the applicable Services, or as otherwise made reasonably available by PCS.

“**PCS Group**” means PCS and its Affiliates engaged in the Processing of Personal Data.

“**Sub-processor**” means any Processor engaged by PCS or a member of the PCS Group.

“**UK GDPR**” has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the UK Data Protection Act 2018.

2. PROCESSING OF PERSONAL DATA

2.1. Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is a

Controller or a Processor, PCS is a Processor and that PCS or members of the PCS Group will engage Sub-processors pursuant to the requirements set forth in section 5 “Sub-processors” below.

- 2.2. **Customer’s Processing of Personal Data.** Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including any applicable requirement to provide notice to Data Subjects of the use of PCS as Processor as well as the use of Anonymous Data by PCS Group, as provided in the Agreement (including where the Customer is a Processor, by ensuring that the ultimate Controller does so). For the avoidance of doubt, Customer’s instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer specifically acknowledges and agrees that its use of the Services will not violate the rights of any Data Subject, including those that have opted-out from sales or other disclosures of Personal Data, to the extent applicable under Data Protection Laws and Regulations.
- 2.3. **PCS’s Processing of Personal Data.** PCS shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Customer’s documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement. PCS Group may also use Personal Data to derive Anonymous Data for the purposes set forth in the Agreement.
- 2.4. **Details of the Processing.** The subject-matter of Processing of Personal Data by PCS is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 (Details of the Processing) to this DPA.
- 2.5. **Customer Instructions.** PCS shall inform Customer immediately (i) if, in its opinion, an instruction from Customer constitutes a breach of the UK and/or (ii) if PCS is unable to follow Customer’s instructions for the Processing of Personal Data.

3. RIGHTS OF DATA SUBJECTS

PCS shall, to the extent legally permitted, promptly notify Customer of any complaint, dispute or request it has received from a Data Subject such as a Data Subject’s right of access, right to rectification, restriction of Processing, erasure (“right to be forgotten”), data portability, object to the Processing, or its right not to be subject to an automated individual decision making, each such request being a “Data Subject Request”. If required by Data Protection Laws and Regulations, Customer shall respond to Data Subject Request in accordance with the Data Protection Laws and Regulations. PCS shall not respond to a Data Subject Request itself, except that Customer authorizes PCS to redirect the Data Subject Request as necessary to allow Customer to respond directly. Taking into account the nature of the Processing, PCS shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Customer’s obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, PCS shall upon Customer’s request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent PCS is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from PCS’s provision of such assistance.

4. PCS PERSONNEL

- 4.1. **Confidentiality.** PCS shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data and have executed written confidentiality agreements. PCS shall ensure that such confidentiality obligations survive the termination of the personnel engagement.
- 4.2. **Reliability.** PCS shall take commercially reasonable steps to ensure the reliability of any PCS personnel engaged in the Processing of Personal Data.
- 4.3. **Limitation of Access.** PCS shall ensure that PCS’s access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.
- 4.4. **Data Protection Officer.** Members of the PCS Group have appointed a data protection officer. The appointed person may be reached at legal@personcenteredsoftware.com.

5. SUB-PROCESSORS

- 5.1. **Appointment of Sub-processors.** Customer acknowledges and agrees that (a) PCS’s Affiliates may be retained as Sub-processors; and (b) PCS and PCS’s Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. PCS or an PCS Affiliate has entered into a written agreement with each Sub-processor containing, in substance, data protection obligations no less protective than those in the Agreement with respect to the protection of Customer Data and/or Professional Services Data to the extent applicable to the nature of the Services provided by such Sub-processor.

- 5.2. List of Current Sub-processors and Notification of New Sub-processors.** The current list of Sub-processors engaged in Processing Personal Data for the performance of each applicable Service, including a description of their processing activities and countries of location, is listed under the Infrastructure and Sub-processor Documentation which can be found on PCS's Trust and Compliance webpage at <https://personcentredsoftware.com/legal/trust-and-compliance-documentation> ("Infrastructure and Sub-processor Documentation"). Customer hereby consents to these Sub-processors, their locations and processing activities as it pertains to their Personal Data. The Infrastructure and Sub-processor Documentation contains a mechanism to subscribe to notifications of new Sub-processors for each applicable Service, and if Customer subscribes, PCS shall provide notification of a new Sub-processor(s) before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services.
- 5.3. Objection Right for New Sub-processors.** Customer may object to PCS's use of a new Sub-processor by notifying PCS promptly in writing within thirty (30) days of receipt of PCS's notice in accordance with the mechanism set out in section 5.2. If Customer objects to a new Sub-processor as permitted in the preceding sentence, PCS will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If PCS is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Customer may terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by PCS without the use of the objected-to new Sub-processor by providing written notice to PCS. PCS will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.
- 5.4. Liability.** PCS shall be liable for the acts and omissions of its Sub-processors to the same extent PCS would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

6. SECURITY

- 6.1. Controls for the Protection of Customer Data & Professional Services Data.** PCS shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data and Professional Services Data), confidentiality and integrity of Customer Data and Professional Services Data, as set forth in the Security and Privacy Documentation. PCS regularly monitors compliance with these measures. PCS will not materially decrease the overall security of the Services during a subscription term.
- 6.2. Cooperation and Audits.** PCS shall make available to Customer such information as is reasonably requested by Customer to demonstrate its compliance with applicable statutory obligations, in a commonly used and machine-readable format, to the extent such information is available to PCS. In cases of official requests of data protection authorities with jurisdiction over the Processing hereunder, or, in case Customer has reasonable grounds to assume that a Customer Data Incident has taken place, Customer may upon at least fourteen (14) days prior written notice to PCS conduct a site visit of the applicable PCS operations center at Customer's expense by a representative of Customer or its independent third party auditor (always not a direct competitor of PCS). Such audits shall be carried out at normal business hours without disrupting the on-going business operations of PCS. PCS may make the audits dependent on the signing of a nondisclosure agreement with PCS.
- 6.3. Data Protection Impact Assessment.** Upon Customer's request, PCS shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligation under Data Protection Laws and Regulations to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to PCS.

7. CUSTOMER DATA INCIDENT NOTIFICATION

- 7.1. PCS responsibilities.** PCS shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data or Professional Services Data, including Personal Data, transmitted, stored or otherwise Processed by PCS or its Sub-processors of which PCS becomes aware (a "Customer Data Incident"). PCS shall make reasonable efforts to identify the cause of such Customer Data Incident and take such steps as PCS deems necessary and reasonable to remediate the cause of such a Customer Data Incident to the extent the remediation is within PCS's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's Users.
- 7.2. Customer responsibilities.** If required under Data Protection Laws and Regulations, Customer shall notify Customer Data Incident to the relevant authorities or Data Subjects in accordance with the Data Protection Laws and Regulations.

8. RETURN AND DELETION OF CUSTOMER DATA

The procedure is set forth in Section 2.2 of the Agreement.

9. UK&EU SPECIFIC TERMS

- 9.1. Definitions.** "GDPR" means 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, and repealing Directive 95/46/EC (General Data Protection Regulation), including as implemented or adopted under the laws of EEA member states.

- 9.2. GDPR & UK GDPR.** PCS will Process Personal Data in accordance with the GDPR and UK GDPR requirements directly applicable to PCS's provision of its Services.
- 9.3. Data Transfers.** PCS shall ensure that the transfer of Personal Data which are undergoing Processing or are intended for Processing after transfer to a third country shall take place only if such transfer meets the conditions outlined in the GDPR and UK GDPR, specifically Chapter V.

10. AUTHORIZED AFFILIATES

- 10.1. Contractual Relationship.** The parties acknowledge and agree that, by executing the Agreement, Customer enters into this DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between PCS and each such Authorized Affiliate subject to the provisions of the Agreement and this section 10 and section 11. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement, and is a party only to this DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.
- 10.2. Communication.** The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with PCS under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.
- 10.3. Rights of Authorized Affiliates.** Where an Authorized Affiliate becomes a party to this DPA with PCS, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

10.3.1 Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against PCS directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA, not separately for each Authorized Affiliate individually, but in a combined manner for itself and all of its Authorized Affiliates together (as set forth, for example, in section 10.3.2, below).

10.3.2 The parties agree that the Customer that is the contracting party to the Agreement shall, when carrying out an On-Site Audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on PCS and its Sub-Processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of itself and all of its Authorized Affiliates in one single audit.

11. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and PCS, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

For the avoidance of doubt, PCS's and its Affiliates' total liability for all claims from Customer and all of its Authorized Affiliates arising out of or related to the Agreement and all DPAs shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Customer and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA.

List of Schedules

Schedule 1: Details of the Processing

SCHEDULE 1 - DETAILS OF THE PROCESSING

Nature and Purpose of Processing

PCS will Process Personal Data as necessary to perform the Services or Professional Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Customer in its use of the Services or Professional Services.

Duration of Processing

Subject to Section 8 of the DPA, PCS will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Categories of Data Subjects

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Customer's staff
- Customer's clients, their relatives and visitors
- Customer's Users authorized by Customer to use the Services

Type of Personal Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- For all categories of data subjects - First and last name, ID data, Contact information (email, phone, physical address), photos
- For Customer's staff and Users - Position and employer.
- For Customer's clients – Details of care provision, demographic data and NHS number
 - Optionally: Race/ethnic origin, demographic data, data about children, physical or mental health, sex, life/sexual orientation, biometric/genetic data, religious and philosophical beliefs
- Usage data – IP Address