Data Processing Agreement

This Data Processing Agreement ("DPA") is hereby incorporated into and is governed by the terms and conditions including any terms and conditions of SOW Services between Seller and Customer, as applicable (together the "Agreement") and applies to the extent that Seller processes any Personal Information (as defined herein) on behalf of Customer in the provision of Services thereunder. The purpose of this DPA is to set out the rights and obligations of the Parties in respect of the Personal Information processed by Seller in its capacity as a processor or service provider under the Agreement. If there is any inconsistency or .conflict between the terms of the Agreement and this DPA as it relates to the processing of Personal Information on behalf of the Customer by the Seller, this DPA shall prevail.

1. **Definitions**:

   a. "controller," "business," "processor," "service provider," "data subject," "consumer," "process," "sale," "sell," "business purpose," and "supervisory authority" (or any equivalent terms) have the meaning set out under Data Protection Laws.

   b. "California Consumer Privacy Act" or "CCPA" means Title 1.81.5 California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100–1798.199), as amended by the California Privacy Rights Act of 2020, (2020 Cal. Legis. Serv. Proposition 24, codified at Cal. Civ. Code §§ 1798.100 et seq.), and its implementing regulations, each as amended or superseded from time to time.

   c. "European Data Protection Laws" means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as amended or superseded from time to time ("EU GDPR"); the EU GDPR as it forms part of the law of the United Kingdom by virtue of section 3 of the UK European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (together, "UK Data Protection Laws"); and the Swiss Federal Data Protection Act of 19 June 1992 and its Ordinance ("Swiss DPA").

   d. "Data Protection Laws" means applicable laws governing the privacy and security of Personal Information, including, where applicable, and without limitation, European Data Protection Laws and/or CCPA.

   e. "Permitted Purpose" means processing of Personal Information (i) as necessary for the provision of the Services as set forth in greater detail in Schedule 1; (ii) as otherwise permitted by Data Protection Laws in connection with the Services; and (iii) to comply with legal obligations which do not conflict with Data Protection Laws.

   f. "Personal Information" means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household in connection with the Services performed for Customer, including without limitation any information that qualifies as "personal information" or "personal data" under the Data Protection Laws applicable to Seller.

   g. "Restricted Transfer" means (i) where EU GDPR or the Swiss DPA applies, a transfer of Personal Information from the European Economic Area ("EEA") including Switzerland to a country outside of the EEA, which is not the subject of an adequacy determination by the European Commission; and (ii) where UK GDPR applies, a transfer of Personal Information from the United Kingdom to any country which is not subject to adequacy regulations pursuant to Section 17A of the UK Data Protection Act.

   h. "Security Breach" means a breach of security leading to unauthorized disclosure of or access to Personal Information in Seller's possession, custody or control.

   i. "Sensitive Data" means (a) social security number, tax file number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) credit or debit card number (other than the truncated (last four digits) of a credit or debit card); (c) employment, financial, credit, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, information about sexual life or sexual orientation, or criminal record; (e) account passwords; or (f) other information that falls within the definition of "special categories of data," "sensitive data" or "nonpublic personal information" under applicable Data Protection Laws or personal information as defined in appliable data breach notification laws.

   j. "Standard Contractual Clauses" means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementation Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Information to third countries pursuant to the EU GDPR ("EU SCCs"); and (ii) where the UK Data Protection Laws apply, the UK Addendum to the EU Standard Contractual Clauses issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018 (the "UK Addendum").

2. **Scope of DPA**

a. This DPA applies to the extent that Seller will process Personal Information on behalf of Customer in the provision of Services under the Agreement. For the avoidance of doubt, it is the intention of the Parties that Seller be a "service provider," "processor" or "licensee" of Customer when required by applicable Data Protection Laws and that Customer be a "business," "controller" or "licensor" when required by applicable Data Protection Laws.

b. Notwithstanding the foregoing, the Parties acknowledge and agree that Seller will not be required to process any Sensitive Data on behalf of Customer unless explicitly stated in a SOW, in which case the Customer will identify the categories and types of Sensitive Data which will be the subject of the processing in the applicable SOW. Unless the Parties agree that Seller will process Sensitive Data on behalf of Customer in a SOW, Customer will restrict Seller's access to any Sensitive Data under its possession or control.

c. If any Data Protection Law imposes additional or overriding obligations to those set forth in this DPA with respect to processing of Personal Information or requires Customer and Seller to enter into any additional agreements, including data export instruments, or to implement any additional security or organizational security measures to process Personal Information under this DPA, Customer shall ensure that it complies with the applicable Data Protection Law in advance of disclosing any Personal Information subject to such Data Protection Laws and the Parties agree to negotiate such additional obligations, agreements, or security measures in good faith.

3. **Customer's Obligations.**

a. The Parties agree that Customer is responsible for obtaining any consents required by applicable Data Protection Laws, as well as providing and ensuring the accuracy of any notices required to disclose Personal Information to Seller, Seller's Affiliates, or any Seller subcontractor providing Services for use in accordance with the Agreement. Furthermore, Customer warrants that all Personal Information processed by Seller in accordance with these terms has been obtained and provided to Seller in accordance with all applicable laws and ensured that there are lawful grounds for processing any and all Personal Information by Seller, Seller's Affiliates, or any Seller subcontractor providing Services for use in accordance with the Agreement.

b. Customer is fully responsible for its compliance with the Data Protection Laws. If additional cooperation from Seller is required to ensure such compliance, the Parties will negotiate in good faith to address the terms of such cooperation, including reimbursement of Seller costs for such additional services or support with respect thereto.

4. **Seller's Obligations.**

a. Seller shall only process Personal Information for the Permitted Purpose and in accordance with Customer's instructions. Customer acknowledges that Seller is reliant on Customer for instruction as to the extent to which Seller is entitled to use and process Personal Information, and that Seller is not liable for any claim brought by a data subject to the extent that such claim arises from Customer's instructions. Where Data Protection Laws requires Seller to process Personal Information under terms other than those of the Agreement, Seller shall promptly notify Customer of such legal requirement before processing, unless the Data Protection Laws prohibits such disclosure. Where required by Data Protection Laws, Seller shall also notify Customer if Seller determines any of Customer's instructions infringes applicable Data Protection Laws.

b. Schedule 1 hereto sets forth the subject matter, duration, nature and purpose of processing and the categories of Personal Information and data subject types relevant to the processing to fulfil the Permitted Purpose. If and to the extent that the Parties agree pursuant to Section 2(b) hereof that Seller will process Sensitive Data on behalf of Customer, the Parties will identify the additional categories of Personal Information and types of data subjects which will be the subject of the processing in the applicable SOW and any additional restrictions or security measures that need to be applied to the Sensitive Data, if any.

5. **Cooperation.**

a. Upon request, Seller shall provide reasonable cooperation and any necessary assistance to Customer in (i) responding to any legally required inquiries, complaints, or other communication regarding its processing of Personal Information, (ii) any request from a data subject to exercise its rights under Data Protection Law (including access, correction, deletion, portability, as applicable) including by assisting with appropriate technical and organizational measures, and (iii) Customer's obligations under applicable Data Protection Laws including assisting with data impact assessments where applicable, in each case in so far as possible and taking into account the nature of Seller's processing and the Personal Information available to Seller. Seller shall be obliged to provide such assistance only in so far that the Customer cannot respond to such request on its own. Notwithstanding anything to the contrary in the Agreement, Customer is obliged to reimburse Seller for out-of-pocket expenses in connection with such cooperation. Such expenses will be invoiced to Customer in accordance with the Agreement.

b. Seller shall promptly notify Customer of any request, complaint, claim, or other communication received by Seller or a subcontractor from a third-party regarding its processing of Personal Information.

6. **Security Breach**. Seller shall promptly notify Customer in the event Seller discovers or is notified of a Security Breach. Seller shall reasonably cooperate in the investigation of the Security Breach. If and to the extent that the Security Breach is proximately caused by Seller's failure to comply with this DPA Seller will reimburse Customer for its documented and reasonable out-of-pocket costs of providing legally required notifications to those individuals whose Personal Information was the subject of the Security Breach, and/or the media or regulatory authorities, as applicable. Any limitation of liability set forth in the Agreement will apply to this DPA and reimbursement obligations.

7. **Restricted Transfers**. If and to the extent that performance of any Services requires the transfer of Personal Information from Customer to Seller which is a Restricted Transfer the Parties agree that the applicable terms attached as Schedule 3 to this DPA shall govern such Restricted Transfer. Seller will not participate in (nor permit any sub-processor to participate in) any other Restricted Transfer unless made in compliance with European Data Protection Laws. Any other transfer of Personal Information from either Party outside of the country in which the Services are being provided and which is not a Restricted Transfer shall be in compliance with applicable Data Protection Laws.

8. **Security**.

    a. Seller shall implement and maintain an information security program that establishes reasonable and appropriate technical, organizational, and physical safeguards designed to protect Personal Information in its control or possession, taking into account the nature of Seller's processing. A description of Seller's information security program is attached as Schedule 2 to this DPA. To the extent required by applicable Data Protection Laws, upon request, Seller shall make available to Customer information reasonably necessary to demonstrate compliance with this obligation.

    b. The technical, organization and physical measures listed in Schedule 2 are subject to technological process and advancement. As such, Seller may implement alternative, adequate measures, which meet or exceed the security level of the measures described in Schedule 2 and will notify Customer only if Seller's implementation of alternative security measures results in a material diminution of the security of Seller's overall information security program.

    c. Upon Customer's written request on an annual basis, Seller shall provide customer-facing documentation on the current state of Seller's information security program and/or third-party certification or security assessment documentation.

9. **Sub-processors**. The parties agree that Seller may subcontract its obligations to subcontractors as necessary to perform the Services under the Agreement. Seller shall remain responsible for subcontractors' performance under the Agreement and shall enter into an agreement with subcontractors that impose materially the same obligations as set forth in this DPA. Seller also agrees that any Personnel or subcontractors who have access to Personal Information are bound to process Personal Information in accordance with Seller's instructions and are subject to obligations to maintain confidentiality.

10. **Return or Destruction**. Notwithstanding any other provision of the Agreement to the contrary, upon termination of the Agreement or otherwise at Customer's written request, Seller shall, at the direction of Customer, either return or delete Personal Information hosted or stored on its systems in the provision of Services unless required by law, rule or regulation, or requested by any judicial, administrative, governmental or regulatory authority to retain or if return or destruction would otherwise involve disproportionate efforts under the circumstances. After Personal Information has been deleted from Seller's active systems, it may continue to exist in backups and logs for a period of time until these are overwritten in the normal course of business and in accordance with Seller's data retention and destruction policies.

11. **CCPA Provisions**

    a. Seller agrees that it will not: (1) sell or share Personal Information as those terms are defined by Data Protection Laws; (2) combine Personal Information received from or on behalf of Customer with Personal Information received from other sources or the data subject unless otherwise permitted to do so under Data Protection Laws; or (3) process Personal Information for any purposes outside the direct business relationship with Customer or as permitted by Data Protection Laws, in each case unless otherwise instructed by Customer to do so. Seller certifies that it understands the foregoing restrictions and will comply with them.

    b. Seller further agrees to: (1) provide at least the same level of privacy protection with respect to the Personal Information as is required by applicable Data Protection Laws; (2) cooperate with reasonable and appropriate assessments or reviews that are legally required, and are necessary to enable Customer to confirm that Seller is processing Personal Information in a manner consistent with Customer's obligations under Data Protection Laws; (3) notify Customer in writing if it can no longer comply with Data Protection Laws with respect to its processing of Personal Information; and (4) permit Customer to cease the transfer of Personal Information to Seller or limit any access by Seller to Personal Information in order to mitigate and remediate any unauthorized use of Personal Information or otherwise take any reasonable steps to stop any unauthorized use of Personal Information, all upon reasonable notice to Seller.

c. Notwithstanding the foregoing, to the extent expressly set forth in the Agreement, Seller shall have the right to retain, use or disclose de-identified or aggregated data derived from Personal Information ("Aggregated Data"), provided that (1) Aggregated Data shall not include any Personal Information; (2) Seller adopt reasonable measures to prevent such Aggregated Data from being used to infer information about, or otherwise being linked to, a particular natural person or household; (3) publicly commits to maintain and use such Aggregated Data in a deidentified form and to not attempt to re-identify the Aggregated Data, except that Seller may attempt to re-identify the data solely for the purpose of determining whether its deidentification processes are compliant with Data Protection Laws.

Schedule 1

Data Processing Description

A. List of Parties

Data Exporter(s):

Name:	Customer or Customer Affiliate identified in applicable SOW
Address:	As set forth in the in the applicable SOW or otherwise provided to Seller
Contract person's name, position and contact details	As set forth in the applicable SOW or otherwise provided to Seller
Activities relevant to the data transferred under these Clauses:	See Section B
Role (controller/processor):	Controller

Data importer(s):

Name:	Seller or Seller Affiliate identified in applicable SOW
Address:	As set forth in the in the applicable SOW or otherwise provided to Customer
Contract person's name, position and contact details	Clay Ullrick Director – Senior Counsel, Global Ethics & Compliance personaldatainquiry@cdw.com
Activities relevant to the data transferred under these Clauses:	See Section B
Role (controller/processor):	Processor

B. Description of Processing/Transfer

Subject Matter, Nature and Purpose of Processing	Processing as reasonably necessary and proportionate to perform the Services on behalf of Customer pursuant to the Agreement for business purposes and in accordance with the DPA. The foregoing includes project based professional and managed Services (including, but not limited to, configuration, implementation, assessment, staff augmentation, unified communications, hosted and network services) maintaining or servicing accounts, providing storage and other types of processing of Personal Information as necessary to provide the Services.
Categories of Data Subjects	Customers' employees and customers.
Types of Personal Information	Name, address (physical), email, phone number, IP address, system access/usage/authorization data Other non-Sensitive Data **No processing of Sensitive Data or any special categories is intended; if and to the extent that processing of the foregoing are necessary under a specific Statement of Work, then the parties will update the applicable SOW. Customer is solely responsible for determining and notifying Seller of such processing and additional restrictions and/or security measures (if any) that are needed to be applied to the Sensitive Data transferred by Customer.**
Duration	Continuous over the term of the Agreement plus the limited time following its termination in accordance with Section 10.

Schedule 2

Data Security Statement

Where applicable to the Services provided and for its own infrastructure, CDW implements reasonable and appropriate technical, organizational and physical safeguards designed to protect against unauthorized processing (such as unauthorized access, collection, use, copying, modification, disposal or disclosure, unauthorized, unlawful, or accidental loss, destruction, acquisition, or damage) Customer Personal Information in CDW custody or control.

1. **Standards.** CDW aligns applicable portions of its operations with various data security standards, such as the data security requirements of: (i) Sarbanes-Oxley Act; (ii) the Health Insurance Portability and Accountability Act; (iii) the Payment Card Industry's Data Security Standard; (iv) the General Data Protection Regulation; (v) the Personal Information Protection and Electronic Documents Act; (vi) the ISO/IEC 27001 Information Security Standard; and (vii) the Statement on Standards for Attestation Engagements No. 18.

2. **Security Policies.** CDW will implement, maintain, and monitor, at all times, a comprehensive, written information security program, aligned to industry standards and that contains appropriate administrative, technical, and physical safeguards designed to protect the security, confidentiality, or integrity of Personal Information in CDW custody or control ("Information Security Program") that meets or exceeds the requirements of these Standards and applicable law. Such Information Security Program summary information shall be available for the Customer's review, on the Customer's request. CDW reviews and, as necessary, revises its Information Security Program at least annually and will notify customers if changes to the program negatively impact the level of security provided.

3. **Access Controls.** CDW will maintain appropriate access controls designed to restrict physical and logical access to Personal Information in CDW custody or control to only those necessary for the provision of Services. The controls include, but are not limited to:
    - monitoring and logging physical and logical access to CDW systems that contain Personal Information;
    - reviewing successful and failed access attempts for systems that contain Personal Information to identify potentially malicious activity;
    - ensuring personnel accessing systems that store Personal Information use unique individual access credentials that meet industry standards for password strength; and
    - maintaining a formal program for the periodic review of access and removal of access to for those personnel that no longer require access.

4. **Secure Infrastructure.** CDW maintains a secure infrastructure topology that meets industry standards for:
    - segmentation, ensuring Personal Information is logically separated from CDW data and that of other CDW customers,
    - firewall and network architecture, including considerations for internal and external communications,
    - intrusion detection and prevention,
    - encryption for data at rest and in motion,
    - device hardening and standard configuration, including the removal of system defaults and unused ports and services,
    - malware detection and prevention designed to protect CDW systems, including those that store Personal Information or connect to customer environments, and
    - Security Event and Incident Monitoring, including alerting, response, remediation, and log protection and retention procedures.

5. **Threat Monitoring.** CDW implements industry standard controls to detect or prevent unauthorized devices from connecting to the network that provides Services. Additionally, CDW implements controls for
    - vulnerability awareness, including industry awareness and regular vulnerability scans and penetration testing,
    - vulnerability management, including patch management, and
    - security incident response plans for the identification, escalation, mitigation, and resolution of suspected security incidents.

6. **Training**. CDW requires its employees to attend and complete periodic information security education and awareness training.

Schedule 3 to the DPA

Applicable Standard Contractual Clauses and Supplemental Terms

1. Incorporation of EU Standard Contractual Clauses

The parties agree that the EU SCCs are hereby incorporated by reference into this DPA in accordance with the terms below.

Module 2: Controller to processor module applies when Customer is the EEA-based data exporter and Controller and Seller is the data importer and Processor.

2. EU Standard Contractual Clause Optional Provisions

Where the EU SCCs identify optional provisions (or provisions with multiple options) the following shall apply in the following manner:

a. Clause 7 (Docking Clause) shall apply;
b. In Clause 9(a) (Use of sub-processors) – Option 2 shall apply.
c. In Clause 11(a) (Redress) – the optional provision shall NOT apply;
d. For purposes of Clause 13, the Dutch Data Protection Authority (Autoriteit Persoonsgegevens, AP) shall be deemed the competent supervisory authority;
e. In Clause 17 (Governing Law) – the laws of the Netherlands shall govern; and
f. In Clause 18 (Choice of forum and jurisdiction) - the courts of the Netherlands shall have jurisdiction.
g. Annex I to the SCCs shall be completed with the details set forth in Schedule 1 to the DPA.
h. Annex II to the SCCs shall be completed with the details set forth in Schedule 2 to the DPA (Data Security Statement).

3. Supplementary Terms to Standard Contractual Clauses

a. Documentation and compliance. For the purposes of Clause 8.9(b) the review and audit provisions in the Agreement and DPA shall apply.
b. Notification and Transparency.
    i. The Parties acknowledge and agree that Seller, where required by the EU SCCs to notify the competent supervisory authority, shall first provide Customer with the details of the notification, permitting Customer to have prior written input into the relevant notification where Customer so desires to do, and without delaying the timing of the notification unduly.
    ii. For purposes of Clause 8.3 – Module 2 and Clause 15.1(a), the parties agree and acknowledge that it may not be possible for Seller to make the appropriate communications to data subjects and accordingly, Customer shall (following notification by the data importer) have the option to be the party who makes any communication to the data subject, and Seller shall provide the level of assistance set forth in the DPA.
c. Liability. For the purposes of Clause 12(a), the liability of the Parties shall be limited in accordance with the limitation of liability provisions in the Agreement.
d. Signatories. Notwithstanding the fact that the SCCs are incorporated herein by reference without being signed directly, Seller and Customer each agrees that their execution of the Agreement is deemed to constitute its execution of the SCCs as of the date thereof, and that it is duly authorized to do so on behalf of, and to contractually bind, the Data Exporter or Data Importer (as applicable) accordingly.

4. Swiss Law Provisions

With respect to Personal Information transferred from Switzerland governed by Swiss law:

a. references to the EU, member states and GDPR in the SCCs are amended mutatis mutandis to refer to Switzerland, the Swiss DPA (as it may be updated or replaced from time to time), and the Swiss Federal Data Protection and Information Commissioner; and
b. In Clause 17 (Governing Law) the laws of Switzerland shall govern, and in Clause 18 (Choice of forum and jurisdiction) the courts of Switzerland shall have jurisdiction.

5. UK Addendum

With respect to Personal Information transferred from the United Kingdom governed by UK Data Protection Laws:

a. The information required by Tables 1 – 3 of the template International Data Transfer Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it may be revised from time to time (the "Template UK Addendum") is provided in the Agreement, DPA, and SOW(s).
b. References to the EU, member states and GDPR in the Standard Contractual Clauses are amended mutatis mutandis to refer to the United Kingdom, the UK Data Protection Act 2018 (as it may be updated or replaced from time to time), and the UK Information Commissioner's Office (the "ICO"); and
c. In Clause 17 (Governing Law), the laws of England and Wales shall govern, and in Clause 18 (Choice of forum and jurisdiction), the courts in London, England shall have jurisdiction. A data subject may also bring legal proceedings against the data exporter and/or data importer before appropriate courts in England and Wales.
d. If there is any inconsistency or conflict between UK Data Protection Laws (including the Template UK Addendum) and the SCCs including this UK Addendum, UK Data Protection Laws including the Template UK Addendum will govern data transfers from the United Kingdom. To the extent required by UK Data Protection Laws the Template UK Addendum is incorporated herein.
e. If the meaning of any provision of the SCCs including this section is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
f. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.
g. Although Clause 5 of the SCCs says that the SCCs prevail over all related agreements between the parties, the parties agree that this UK Addendum will supersede other provisions of the SCCs regarding data transfers from the United Kingdom.