NASPO ValuePoint

PARTICIPATING ADDENDUM

DATA COMMUNICATION PRODUCTS & SERVICES (2019-2026)

Led by the State of **Utah**

Master Agreement #: AR3228 Participating Addendum # AR3228

Contractor: **HEWLETT PACKARD ENTERPRISE COMPANY**

Participating Entity: **STATE OF UTAH**

The following products or services are included in this contract portfolio:

All products and accessories listed on the Contractor page of the NASPO ValuePoint website.

Master Agreement Terms and Conditions:

1. Scope: This Addendum covers the ***Data Communication Products and Services*** led by the State of Utah for use by state agencies and other entities located in the Participating State or State Entity authorized by that State's statutes to utilize State contracts with the prior approval of the State's Chief Procurement Official.

2. Pricing: Prices and rates from the Master Agreement shall flow down to this PA. An amendment to this PA is not required when pricing in the Master Agreement is adjusted / updated.

3. Contract Effective Dates: This PA is effective upon final signature of both parties, and expires upon the expiration or termination of the NASPO ValuePoint Master Agreement AR3228. A contract amendment is not necessary in the event of the renewal or extension of the Master Agreement, so long as such renewal/extension was originally provided within the solicitation supporting the master agreement.

4. Order of Precedence: The order of precedence as provided in the NASPO ValuePoint Master Agreement AR3228 Attachment A section 1 applies to this PA.

5. Participation: This Addendum to the NASPO ValuePoint Master Agreement may be used by all state agencies, institutions of higher institution, political subdivisions and other entities authorized to use statewide contracts in the State of Utah. Issues of interpretation and eligibility for participation are solely within the authority of the State Chief Procurement Official.

6. Primary Contacts: The primary contact individuals for this Participating Addendum are as follows (or their named successors):

Contractor

Name:	Nancy Schwarz
Address:	6280 America Center Drive, San Jose, CA 95002
Telephone:	(480) 636-0267
Email:	Nancy.schwarz@hpe.com

Participating Entity

Name:	Solomon Kingston
Address:	3150 State Office Building, Salt Lake City, UT 84114
Telephone:	801-538-3228
Email:	skingston@utah.gov

7. Participating Entity Modifications Or Additions To The Master Agreement

The following terms and conditions will apply to this participating addendum.

1. DEFINITIONS:

a. "Access to Secure Public Facilities, Data, and Technology" means Contractor will (A) enter upon secure premises controlled, held, leased, or occupied by the State of Utah or an Eligible User; (B) maintain, develop, or have access to any deployed hardware, software, firmware, or any other technology, that is in use by the State of Utah or an Eligible User; or (C) have access to or receive any Public Data or Confidential Information during the course of performing this Contract.

b. "Authorized Persons" means the Contractor's employees, officers, partners, Subcontractors or other agents of Contractor who need to access Public Data to enable the Contractor to perform its responsibilities under this Contract.

c. "Confidential Information" means information that is deemed as confidential under applicable record laws. The State of Utah and the Eligible Users reserves the right to identify, during and after this Contract, additional reasonable types of categories of information that must be kept confidential under federal and state laws by Contractor.

d. "Contract" means this State of Utah PA, including the referenced NASPO ValuePoint Master Agreement AR3228, and all referenced attachments and documents incorporated by reference. This Contract may include any purchase orders that result from the parties entering into this Contract.

e. "Contractor" is as defined in the NASPO ValuePoint Master Agreement AR3228 Attachment A section 2.

f. "Data Breach" is as defined in the NASPO ValuePoint Master Agreement AR3228 Attachment A section 2.

g. "Division" means the State of Utah Division of Purchasing.

h. "DTS" means the Department of Technology Services.

i. "Eligible User(s)" means the State of Utah's government departments, institutions, agencies, political subdivisions (i.e., colleges, school districts, counties, cities, etc.), and, as applicable, nonprofit organizations,

agencies of the federal government, or any other entity authorized by the laws of the State of Utah to participate in State Cooperative Contracts will be allowed to use this Contract.

j. "Federal Criminal Background Check" means an in depth background check conducted and processed by the FBI that covers all states. Federal Criminal Background Check reports will show if applicant has had any criminal cases filed against them that violated federal criminal law.

k. "Good" means any deliverable not classified as a Custom Deliverable or Service that Contractor is required to deliver to the Eligible Users under this Contract.

l. "Non-Public Data" means data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the State of Utah and the federal government because it contains information that is exempt by state, federal and local statutes, ordinances, or administrative rules from access by the general public as public information.

m. "Personal Data" is as defined in the NASPO ValuePoint Master Agreement AR3228 Attachment A section 2.

n. "Proposal" means Contractor's response documents, including attachments, to the NASPO ValuePoint Data Communications Products and Services solicitation.

o. "Protected Health Information" (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.

p. "Security Incident" is as defined in the NASPO ValuePoint Master Agreement AR3228 Attachment A section 2.

q. "Services" means the furnishing of labor, time, or effort by Contractor as set forth in this Contract, including but not limited to installation, configuration, implementation, technical support, warranty maintenance, and other support services.

r. "Solicitation" is as defined in the NASPO ValuePoint Master Agreement AR3228 Attachment A section 2.

s. "Public Data" means all Confidential Information, Non-Public Data, Personal Data, and Protected Health Information that is created or in any way originating with the State of Utah or an Eligible User whether such data or output is stored on the State of Utah's or an Eligible User's hardware, Contractor's hardware, or exists in any system owned, maintained or otherwise controlled by the State of Utah, an Eligible User, or by Contractor. Public Data includes any federal data, that the State of Utah or an Eligible User controls or maintains, that is protected under federal laws, statutes, and regulations.

t. "State of Utah" means the State of Utah, in its entirety, including its institutions, agencies, departments, divisions, authorities, instrumentalities, boards, commissions, elected or appointed officers, employees, agents, and authorized volunteers.

2. **CONTRACT JURISDICTION, CHOICE OF LAW, AND VENUE:** This Contract shall be governed by the laws, rules, and regulations of the State of Utah. Any action or proceeding arising from this Contract shall be brought in a court of competent jurisdiction in the State of Utah. Venue shall be in Salt Lake City, in the Third Judicial District Court for Salt Lake County.

3. **LAWS AND REGULATIONS:** At all times during this Contract, Contractor and all the Goods delivered under this Contract will comply with all applicable federal and state constitutions, laws, rules, codes, orders, and regulations, including applicable licensure and certification requirements.

4. **NO WAIVER OF SOVEREIGN IMMUNITY:** In no event shall this Contract be considered a waiver by the Division, an Eligible User, or the State of Utah of any form of defense or immunity, whether sovereign immunity, governmental immunity, or any other immunity based on the Eleventh Amendment to the Constitution of the United States or otherwise, from any claim or from the jurisdiction of any court.

5. **RECORDS ADMINISTRATION:** Record Administration shall be as outlined in the NASPO ValuePoint Master

Agreement AR3228 Attachment A section 29.

6. **CERTIFY REGISTRATION AND USE OF EMPLOYMENT "STATUS VERIFICATION SYSTEM":** This Status Verification System, also referred to as "E-verify", requirement only applies to contracts issued through a Request for Proposal process and to sole sources that are included within a Request for Proposal.

   (1) Contractor certifies as to its own entity, under penalty of perjury, that Contractor has registered and is participating in the Status Verification System to verify the work eligibility status of Contractor's new employees that are employed in the State of Utah in accordance with applicable immigration laws including Section 63G-12-302, Utah Code, as amended.

   (2) Contractor shall require that the following provision be placed in each subcontract at every tier: "The subcontractor shall certify to the main (prime or general) contractor by affidavit that the subcontractor has verified through the Status Verification System the employment status of each new employee of the respective subcontractor, all in accordance with applicable immigration laws including Section 63G-12-302, Utah Code, as amended, and to comply with all applicable employee status verification laws. Such affidavit must be provided prior to the notice to proceed for the subcontractor to perform the work."

   (3) Contractor's failure to comply with this section will be considered a material breach of this Contract.

   (4) Contractor shall protect, indemnify, and hold harmless the Division, the Eligible Users, and the State of Utah, and anyone that the State of Utah may be liable for, against any claim, damages, or liability arising out of or resulting from violations of the above Status Verification System Section whether violated by employees, agents, or contractors of the following: (a) Contractor; (b) Subcontractor at any tier; and/or (c) any entity or person for whom the Contractor or Subcontractor may be liable.

7. **CONFLICT OF INTEREST:** Contractor represents that none of its officers or employees are officers or employees of the State of Utah, unless disclosure has been made to the Division.

8. **CONFLICT OF INTEREST WITH STATE EMPLOYEES:** Contractor agrees to comply and cooperate in good faith will all conflict of interest and ethic laws including Section 63G-6a-2404, Utah Procurement Code, as amended.

9. **INDEPENDENT CONTRACTOR:** Contractor's legal status is that of an independent contractor, and in no manner shall Contractor be deemed an employee or agent of the Division, the Eligible Users, or the State of Utah, and therefore is not entitled to any of the benefits associated with such employment. Contractor, as an independent contractor, shall have no authorization, express or implied, to bind the Division, the Eligible Users, or the State of Utah to any agreements, settlements, liabilities, or understandings whatsoever, and agrees not to perform any acts as an agent for the Division, the Eligible Users, or the State of Utah. Contractor shall remain responsible for all applicable federal, state, and local taxes, and all FICA contributions.

10. **CONTRACTOR ACCESS TO SECURE Public FACILITIES, PUBLIC DATA, AND TECHNOLOGY:** An employee of Contractor or a Subcontractor may be required to complete a Federal Criminal Background Check, if said employee of Contractor or a Subcontractor will have Access to Secure Public Facilities, Public Data, and Technology. Contractor shall provide the Eligible User with sufficient personal information (at Contractor's own expense) so that a Federal Criminal Background Check may be completed by the Eligible User, at the Eligible User's expense. The Eligible User will also provide Contractor with a Disclosure Form and Confidentiality Agreement which must be filled out by Contractor and returned to the Eligible User. Additionally, each employee of Contractor or a Subcontractor, who will have Access to Secure Public Facilities, Public Data, and Technology, will be scheduled by the Eligible User to be fingerprinted, at a minimum of one week prior to having such access. At the time of fingerprinting, said employee of Contractor or a Subcontractor will disclose, in full, any past record of felony or misdemeanor convictions. The Eligible User is authorized to conduct a Federal Criminal Background Check based upon the fingerprints and personal information provided. The Eligible User may use this same information to complete a Name Check in the Utah Criminal Justice Information System (UCJIS) every two years and reserves the right to revoke Access to Secure State Facilities, Data, and Technology granted in the event of any negative results. Contractor agrees to notify the Eligible User if an arrest or conviction of any employee of Contractor or a Subcontractor that has Access to Secure Public Facilities, Public Data and Technology occurs during this Contract. Contractor, in executing any duty or exercising any right under this Contract, shall not cause or permit any of its employees or employees of a Subcontractor (if any) who have been convicted of a felony or misdemeanor to have Access to Secure Public Facilities, Public Data, and Technology. A felony and misdemeanor

are defined by the laws of the State of Utah, regardless of where the conviction occurred.

11. **DRUG-FREE WORKPLACE:** Contractor agrees to abide by the Eligible User's drug-free workplace policies while on the Eligible User's or the State of Utah's premises.

12. **CODE OF CONDUCT:** If Contractor is working at facilities controlled or owned by the Eligible User, Contractor agrees to comply with the applicable customer policies that are relevant to Contractor's attendance at customer's site or use of customer IT and facilities, subject to the following: (a) customer will provide Contractor with written details of steps required to comply with applicable policies in advance of the performance; and (b) if policy compliance cannot reasonably be achieved by Contractor consistent with the scope or pricing of the Contract, the parties will amend the Contract as necessary.

13. **INDEMNITY CLAUSE:** Indemnity shall be as outlined in the NASPO ValuePoint Master Agreement AR3228 Attachment A section 39.

14. **EMPLOYMENT PRACTICES:** Contractor agrees to abide by the following employment laws: (i)Title VI and VII of the Civil Rights Act of 1964 (42 U.S.C. 2000e) which prohibits discrimination against any employee or applicant for employment or any applicant or recipient of services, on the basis of race, religion, color, or national origin; (ii) Executive Order No. 11246, as amended, which prohibits discrimination on the basis of sex; (iii) 45 CFR 90 which prohibits discrimination on the basis of age; (iv) Section 504 of the Rehabilitation Act of 1973, or the Americans with Disabilities Act of 1990 which prohibits discrimination on the basis of disabilities; and (v) Utah's Executive Order 2019-1, dated February 5, 2019, which prohibits unlawful harassment in the work place. Contractor further agrees to abide by any other laws, regulations, or orders that prohibit the discrimination of any kind of any of Contractor's employees.

15. **SEVERABILITY:** A declaration or order by any court that any provision of this Contract is illegal and void shall not affect the legality and enforceability of any other provision of this Contract, unless the provisions are mutually dependent.

16. **AMENDMENTS:** This Contract may only be amended by the mutual written agreement of the parties, which amendment will be attached to this Contract.

17. **DEBARMENT:** Contractor certifies that it is not presently nor has ever been debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this Contract, by any governmental department or agency, whether international, national, state, or local. Contractor must notify the Division within thirty (30) days if debarred, suspended, proposed for debarment, declared ineligible or voluntarily excluded from participation in any contract by any governmental entity during this Contract.

18. **TERMINATION:** This Contract may be terminated, with cause by either party, in advance of the specified expiration date, upon written notice given by the other party. The party in violation will be given fifteen (15) calendar days after written notification to correct and cease the violations, after which this Contract may be terminated for cause immediately and subject to the remedies below. This Contract may also be terminated without cause (for convenience), in advance of the specified expiration date, by the Division, upon sixty (60) days written termination notice being given to the other party. The State or Participating Entity or Eligible User will pay for equipment and software ordered, delivered, and accepted prior to the date of termination.

    If Services apply to this Contract, then Contractor shall be compensated for the Services properly performed under this Contract up to the effective date of the notice of termination. Contractor agrees that in the event of such termination for cause or without cause, Contractor's sole remedy and monetary recovery from the Division, the Eligible Users, or the State of Utah is limited to full payment for all work properly performed as authorized under this Contract up to the date of termination as well as any reasonable monies owed as a result of Contractor having to terminate other contracts necessarily and appropriately entered into by Contractor pursuant to this Contract.

19. **SUSPENSION OF WORK:** Should circumstances arise which would cause the Division to suspend Contractor's responsibilities under this Contract, but not terminate this Contract, this will be done by formal written notice pursuant to the terms of this Contract. Contractor's responsibilities may be reinstated upon advance formal written notice from the Division.

20. **NONAPPROPRIATION OF FUNDS, REDUCTION OF FUNDS, OR CHANGES IN LAW:** Upon thirty (30) days written notice delivered to the Contractor, this Contract may be terminated in whole or in part at the sole discretion

of the Division or an Eligible User, if it is reasonably determined that: (i) a change in Federal or State legislation or applicable laws materially affects the ability of either party to perform under the terms of this Contract; or (ii) that a change in available funds affects an Eligible User's ability to pay under this Contract. A change of available funds as used in this paragraph, includes, but is not limited to, a change in Federal or State funding, whether as a result of a legislative act or by order of the President or the Governor.

If a written notice is delivered under this section, the Eligible User will reimburse Contractor for the Goods or Services properly ordered until the effective date of said notice. The Eligible User will not be liable for any performance, commitments, penalties, or liquidated damages that accrue after the effective date of said written notice.

21. **SALES TAX EXEMPTION:** The Goods, Custom Deliverables, or Services being purchased by the Eligible Users under this Contract are being paid from the Eligible User's funds and used in the exercise of the Eligible User's essential function as an Eligible User. The Eligible User will provide Contractor with a copy of its sales tax exemption number upon request. It is the Contractor's responsibility to request the sales tax exemption number from the Eligible User.

22. **TITLE AND OWNERSHIP WARRANTY:** Contractor warrants, represents and conveys full ownership, clear title free of all liens and encumbrances to any Good delivered to the Eligible Users under this Contract, unless otherwise specified in the Order. Contractor fully indemnifies the Eligible Users for any loss, damages or actions arising from a breach of this warranty without limitation.

23. **HARDWARE WARRANTY:** Hardware warranty shall be as outlined in the NASPO ValuePoint Master Agreement AR3228 Attachment A section 18.

24. **SOFTWARE WARRANTY:** Software warranty shall be as outlined in the NASPO ValuePoint Master Agreement AR3228 Attachment A section 18.

25. **WARRANTY REMEDIES:** Warranty remedies shall be as outlined in the NASPO ValuePoint Master Agreement AR3228 Attachment A section 18.

26. **UPDATES AND UPGRADES:** Contractor grants to the Eligible Users a non-exclusive, non-transferable license to use upgrades and updates provided by Contractor during the term of this Contract. Such upgrades and updates are subject to the terms of this Contract. The Eligible Users shall download, distribute, and install all updates as released by Contractor during this Contract, and Contractor strongly suggests that the Eligible Users also download, distribute, and install all upgrades as released by Contractor during this Contract.

27. **BUG FIXING AND REMOTE DIAGNOSTICS:** Contractor shall use commercially reasonable efforts to provide work-around solutions or patches to reported software problems. With an Eligible User's prior written authorization, Contractor may perform remote diagnostics to work on reported problems, subject to Contractor's obligation of this Contract. In the event that an Eligible User declines remote diagnostics, Contractor and the Eligible User may agree to on-site technical support, subject to the terms of this Contract.

28. **TECHNICAL SUPPORT AND MAINTENANCE:** If technical support and maintenance is a part of the Goods or Custom Deliverables that Contractor provides under this Contract, Contractor will use commercially reasonable efforts to respond, in a reasonable time, when technical support or maintenance requests regarding the Goods or Custom Deliverables are made to Contractor.

29. **SECURE PROTECTION AND HANDLING OF PUBLIC DATA:** If Contractor is given Public Data as part of this Contract, the protection of Public Data shall be an integral part of the business activities of Contractor to ensure that there is no inappropriate or unauthorized use of Public Data. To the extent that Contractor is given Public Data, Contractor shall safeguard the confidentiality, integrity and availability of the Public Data and comply with the following conditions outlined below. Eligible Users reserve the right to verify Contractor's adherence to the following conditions to ensure they are met during the life of the contract:

    1. **Network Security**: Contractor agrees at all times to maintain network security that - at a minimum - includes: network firewall provisioning, intrusion detection, and regular third party penetration testing. Contractor also agrees to maintain network security that conforms to one of the following:

(1) Those standards the State of Utah applies to its own network, found outlined in *DTS Policy 5000-0002 Enterprise Information Security Policy* (copy available upon request);

(2) Current standards set forth and maintained by the National Institute of Standards and Technology, includes those at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf; or

(3) Any generally recognized comparable standard that Contractor then applies to its own network and approved by DTS in writing.

2. **Public Data Security:** Contractor agrees to protect and maintain the security of Public Data with protection that is at least as good as or better than that maintained by the Contractor's Data Privacy and Security Attachment to this Contract. These security measures included but are not limited to maintaining secure environments that are patched and up to date with all appropriate security updates as designated (ex. Microsoft Notification). Eligible User reserves the right to determine if Contractor's level of protection adequately meets the Eligible User's security requirements.

3. **Public Data Transmission**: Contractor agrees that any and all transmission or exchange of system application data with the Eligible Users and State of Utah and/or any other parties expressly designated by the State of Utah, shall take place via secure means (ex. HTTPS or FTPS).

4. **Public Data Storage**: Contractor agrees that all Public Data will be stored and maintained in data centers in the United States. Contractor agrees that no Public Data at any time will be processed on or transferred to any portable or laptop computing device or any portable storage medium, except for devices that are used and kept only at Contractor's United States data centers, unless such medium is part of the Contractor's designated backup and recovery process. Contractor shall permit its employees and Subcontractors to access non-Public Data remotely only as required to provide technical support and general Order administration. Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model.

5. **Public Data Encryption**: Contractor agrees to store all State of Utah data provided to Contractor as part of its designated backup and recovery process in encrypted form, using no less than 128 bit key.

6. **Password Protection**: Contractor agrees that any portable or laptop computer that has access to the Eligible Users or State of Utah networks, or stores any Public Data is equipped with strong and secure password protection.

7. **Public Data Re-Use:** Contractor agrees that any and all data exchanged shall be used expressly and solely for the purpose enumerated in this Contract. Contractor further agrees that no Public Data of any kind shall be transmitted, exchanged, or otherwise passed to other Contractors or interested parties except on a case-by-case basis as specifically agreed to in writing by the Eligible Users.

8. **Public Data Destruction**: The Contractor agrees that upon expiration or termination of this Contract it shall erase, destroy, and render unreadable all Public Data from all non-state computer systems and backups, and certify in writing that these actions have been completed within thirty (30) days of the expiration or termination of this Contract or within seven (7) days of the request of the Eligible User, whichever shall come first, unless the Eligible User provides Contractor with a written directive. It is understood by the parties that the Eligible User's written directive may request that certain data be preserved in accordance with applicable law.

9. **Services Shall be Performed within United States.** Contractor agrees that all of the Services related to Public Data that it provides to the Eligible Users will be performed by Contractor and Subcontractor(s) within the borders and jurisdiction of the United States. Notwithstanding, Contractor shall permit its employees and Subcontractors to access Public Data remotely only as required to provide technical support and general Order administration. Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model.

30. SECURITY INCIDENT OR DATA BREACH NOTIFICATION: Contractor shall within 48 hours, inform an Eligible User of any Security Incident or Data Breach of Eligible User Public Data.

1. **Incident Response**: Contractor may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement and seeking external expertise as mutually agreed upon, defined by law or contained in this Contract. Discussing Security Incidents with the Eligible User should be handled on an urgent as-needed basis, as part of Contractor's communication and mitigation processes, defined by law or contained in this Contract.

2. **Security Incident Reporting Requirements**: Contractor shall report a Security Incident to the Eligible User within 48 hours if Contractor reasonably believes there has been a Security Incident.

3. **Breach Reporting Requirements**: If Contractor has actual knowledge of a confirmed Data Breach that affects the security of any Public Data that is subject to applicable data breach notification law, Contractor shall: (a) promptly notify the Eligible User within 48 hours or sooner, unless shorter time is required by applicable law; (b) take commercially reasonable measures to address the Data Breach in a timely manner; and (c) be responsible for its Data Breach responsibilities, as provided in the next Section.

31. DATA BREACH RESPONSIBILITIES: This Section only applies when a Data Breach occurs. Contractor agrees to comply with all applicable laws that require the notification of individuals in the event of a Data Breach or other events requiring notification in accordance with DTS Policy 5000-0002 Enterprise Information Security Policy (copy available upon request). In the event of a Data Breach or other event requiring notification under applicable law (Utah Code § 13-44-101 thru 301 et al), Contractor shall: (a) cooperate with the Eligible User by sharing information relevant to the Data Breach; (b) promptly implement necessary remedial measures, if necessary; (c) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in relation to the Data Breach; and (d) in accordance with applicable laws indemnify, hold harmless, and defend DTS and the State of Utah against any claims, damages, or other harm related to such Data Breach. If the Data Breach requires public notification, all communication shall be coordinated with the Eligible User. Contractor shall be responsible for all notification and remedial costs and damages.**32. STATE INFORMATION TECHNOLOGY POLICIES:** If Contractor is providing an Executive Branch Agency of the State of Utah with Goods or Custom Deliverables it is important that contractors follow the same policies and procedures that DTS follows for their own internally developed goods and deliverables to minimize security risk, ensure applicable State and Federal laws are followed, address issues with accessibility and mobile device access, and prevent outages and data breaches within the State of Utah's environment. Contractor agrees to comply with the following DTS Policies which are available upon request:

1. **DTS Policy 4000-0001, Enterprise Application and Database Deployment Policy**: The Enterprise Application and Database Deployment Policy requires any Contractor developing software for the State to develop and establish proper controls that will ensure a clear separation of duties between developing and deploying applications and databases to minimize security risk; to meet due diligence requirements pursuant to applicable state and federal regulations; to enforce contractual obligations; and to protect the State's electronic information and information technology assets.
2. **DTS policy 4000-0002, Enterprise Password Standards Policy**: Any Contractor developing software for the State must ensure it is built to follow the password requirements outlined in the Enterprise Password Standards Policy.
3. **DTS Policy 4000-0003, Software Development Life Cycle Policy**: The Software Development Life Cycle Policy requires any Contractor developing software for the State to work with DTS in implementing a Software Development Lifecycle (SDLC) that addresses key issues of security, accessibility, mobile device access, and standards compliance.
4. **DTS Policy 4000-0004, Change Management Policy**: Per the Change Management Policy, any Goods or Custom Deliverables furnished or Services performed by Contractor which have the potential to cause any form of outage or to modify DTS's or the State of Utah's infrastructure must be reviewed by the DTS Change Management Committee. Following this notification, any outages or Data Breaches which are a direct result of Contractor's failure to comply with DTS instructions and policies following notification will result in Contractor's liability for any and all damages resulting from or associated with the outage or Data Breach.

33. PUBLIC INFORMATION: Contractor agrees that this Contract, any related purchase orders, related invoices, related pricing lists, and the Proposal will be public documents, and may be available for distribution in accordance with the State of Utah's Government Records Access and Management Act (GRAMA). Contractor gives the Division, the Eligible Users, and the State of Utah express permission to make copies of this Contract, any related purchase orders, related invoices, related pricing lists, and Proposal in accordance with GRAMA. The permission to make copies as noted will take precedence over any statements of confidentiality, proprietary information, copyright information or similar notation. The Division, the Eligible Users, or the State of Utah will not inform Contractor of any request for a copy of this Contract, including any related purchase orders, related invoices, related pricing lists, or the Proposal.

34. DELIVERY: Delivery shall be as outlined in the NASPO ValuePoint Master Agreement AR3228 Attachment A section 14.

35. ELECTRONIC DELIVERY: Contractor may electronically deliver any Good or Custom Deliverable to Eligible Users or provide any Good and Custom Deliverable for download from the Internet, if approved in writing by the Eligible Users. Contractor should take all reasonable and necessary steps to ensure that the confidentiality of those electronic deliveries is preserved in the electronic delivery process, and are reminded that failure to do so may constitute a breach of obligations owed to the Eligible Users under this Contract. Contractor warrants that all electronic deliveries will be free of known, within reasonable industry standards, malware, bugs, Trojan horses, etc. Any electronic delivery that includes Public Data that Contractor processes or stores must be delivered within the specifications of this Contract.

36. ACCEPTANCE PERIOD: The acceptance period shall be as outlined in the NASPO ValuePoint Master Agreement AR3228 Attachment A section 16.

37. ORDERING AND INVOICING: Ordering and invoicing shall be as outlined in the NASPO ValuePoint Master Agreement AR3228 Attachment A section 13.

38. PROMPT PAYMENT DISCOUNT: Contractor may quote a prompt payment discount based upon early payment. Contractor shall list payment discount terms on invoices. The prompt payment discount will apply to payments made with purchasing cards and checks. The date from which discount time is calculated will be the date a correct invoice is received.

39. PAYMENT:

1. Payments will be made within thirty (30) days from a correct invoice is received. After sixty (60) days from the date a correct invoice is received by the appropriate State official, the Contractor may assess interest on overdue, undisputed account charges up to a maximum of the interest rate paid by the IRS on taxpayer refund claims, plus two percent, computed similarly as the requirements of Section 15-6-3, Utah Prompt Payment Act of Utah Code, as amended. The IRS interest rate is adjusted quarterly, and is applied on a per annum basis, on the invoice amount that is overdue.

2. Unless otherwise stated in this Contract, all payments to Contractor will be remitted by mail, by electronic funds transfer, or by the Eligible User's purchasing card (major credit card). The Division will not allow Contractor to charge electronic payment fees of any kind.

3. The acceptance by Contractor of final payment without a written protest filed with the Eligible User within ten (10) working days of receipt of final payment shall release the Eligible User, the Division, and the State of Utah from all claims and all liability to Contractor for fees and costs pursuant to this Contract.

4. Contractor agrees that if during, or subsequent to the Contract an audit determines that payments were incorrectly reported or paid by the Eligible Users to Contractor, then Contractor shall, upon written request, immediately refund to the Eligible Users any such overpayments.

40. INDEMNIFICATION – INTELLECTUAL PROPERTY: Indemnification – Intellectual Property shall be as outlined in the NASPO ValuePoint Master Agreement AR3228 Attachment A section 39.b.

41. OWNERSHIP IN INTELLECTUAL PROPERTY: The parties each recognize that each has no right, title, or interest, proprietary or otherwise, in or to the name or any logo, or intellectual property owned or licensed by the other. Each agree that, without prior written consent of the other or as described in this Contract, it shall not use the name, any logo, or intellectual property owned or licensed by the other.

42. OWNERSHIP IN CUSTOM DELIVERABLES: [reserved as not applicable]

43. OWNERSHIP, PROTECTIN AND USE OF RECORDS: [reserved, HPE is not transferring title of its IP. Ownership of records is specified in Section 41 of the State of Utah PA. Confidentiality of records is covered in Section 46 of the State of Utah PA]

44. PROTECTION, AND USE OF CONFIDENTIAL FEDERAL, STATE, OR LOCAL GOVERNMENT INTERNAL BUSINESS PROCESS AND PROCEDURES. In the event that the Eligible User provides Contractor with confidential federal or state business processes, policies, procedures, or practices, pursuant to this Contract,

Contractor agrees to hold such information in confidence, in accordance with applicable laws and industry standards of confidentiality, and not to copy, reproduce, sell, assign, license, market, transfer, or otherwise dispose of, give, or disclose such information to third parties or use such information for any purpose whatsoever other than the performance of this Contract. The improper use or disclosure by any party of protected internal federal or state business processes, policies, procedures, or practices is prohibited. Confidential federal or state business processes, policies, procedures or practices shall not be divulged by Contractor or its Subcontractors, except for the performance of this Contract, unless prior written consent has been obtained in advance from the Eligible User.

45. **PROTECTION AND RETURN OF DOCUMENTS AND DATA UPON CONTRACT TERMINATION OR COMPLETION:** refer to NASPO ValuePoint Master Agreement AR3228 Attachment A section 30.

46. **CONFIDENTIALITY:** Confidentiality shall be as outlined in the NASPO ValuePoint Master Agreement AR3228 Attachment A section 30.

    Contractor shall be responsible for any breach of this duty of confidentiality contract by any of their officers, agents, subcontractors at any tier, and any of their respective representatives, including any required remedies and/or notifications under applicable law (Utah Code Section 13-44-101 thru 301 et al). Contractor shall indemnify, hold harmless, and defend the Division, the Eligible Users, and State of Utah from claims related to a breach of these confidentiality requirements by Contractor or anyone for whom the Contractor is liable. This duty of confidentiality shall be ongoing and survive the term of this Contract.

47. **ASSIGNMENT/SUBCONTRACT:** Contractor will not assign, sell, transfer, subcontract or sublet rights, or delegate responsibilities under this Contract, in whole or in part, without the prior written approval of the Division.

48. **DEFAULT AND REMEDIES:** Default and Remedies shall be as outlined in the NASPO ValuePoint Master Agreement AR3228 Attachment A section 36.

49. **TERMINATION UPON DEFAULT:** In the event an Order under this Contract is terminated as a result of a default by Contractor, the Eligible User may procure or otherwise obtain, upon such terms and conditions as the Eligible User deems appropriate, Goods, or Services similar to those terminated, and Contractor shall be liable to the Eligible User for any and all direct cover costs and damages arising therefrom, including attorneys' fees, excess costs and fees, and cost of cover, incurred by the Eligible User in obtaining similar Goods, or Services.

50. **FORCE MAJEURE:** Neither party to this Contract will be held responsible for delay or default caused by fire, riot, acts of God and/or war which is beyond that party's reasonable control. The Division and the Eligible Users may immediately terminate this Contract after determining such delay will reasonably prevent successful performance of this Contract.

51. **PROCUREMENT ETHICS:** Contractor understands that a person who is interested in any way in the sale of any supplies, services, products, construction, or insurance to the State of Utah is violating the law if the person gives or offers to give any compensation, gratuity, contribution, loan, or reward, or any promise thereof to any person acting as a procurement officer on behalf of the State of Utah, or who in any official capacity participates in the procurement of such supplies, services, products, construction, or insurance, whether it is given for their own use or for the use or benefit of any other person or organization.

52. **CONTRACTOR'S INSURANCE RESPONSIBILITY**. Contractor's insurance responsibility shall be as outlined in the NASPO ValuePoint Master Agreement AR3228 Attachment A section 28

53. **RESERVED**

54. **CONFLICT OF TERMS:** Contractor terms and conditions that apply must be in writing and attached to this Contract. No other terms and conditions will apply to this Contract including terms listed or referenced on a Contractor's website, terms listed in a Contractor quotation/sales order, purchase orders, etc. In the event of any conflict in the contract terms and conditions, the order of precedence shall be as outlined in the NASPO ValuePoint Master Agreement AR3228 Attachment A section 1.

55. **ENTIRE AGREEMENT:** This Contract shall constitute the entire agreement between the parties, and supersedes any and all other prior and contemporaneous agreements and understandings between the parties, whether oral or written.

56. SURVIVORSHIP: This paragraph defines the specific contractual provisions that will remain in effect after expiration of, the completion of, or termination of this Contract, for whatever reason: (a) Contract Jurisdiction, Choice of Law, and Venue; (b) Secure Protection and Handling of Public Data; (c) Data Breach Responsibilities; (d) Protection, and Use of Confidential Federal, State, or Local Government Internal Business Processes and Procedures; (e) Protection, and Return of Documents and Data Upon Contract Termination or Completion; (f) Confidentiality; (g) Conflict of Terms; and (h) any other terms that by their nature would survive the expiration of, completion, or termination of this contract.

57. WAIVER: The waiver by either party of any provision, term, covenant, or condition of this Contract shall not be deemed to be a waiver of any other provision, term, covenant, or condition of this Contract nor any subsequent breach of the same or any other provision, term, covenant, or condition of this Contract.

58. CONTRACT INFORMATION: During the duration of this Contract, the Division of Purchasing is required to make available contact information of Contractor to the State of Utah Department of Workforce Services. The State of Utah Department of Workforce Services may contact Contractor during the duration of this Contract to inquire about Contractor's job vacancies.

59. COMPLIANCE WITH ACCESSIBILITY STANDARDS: Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973. Contractor must also adhere to Utah Administrative Rule R895-14-1-4-2, which states that vendors proposing IT products and services shall provide Voluntary Product Accessibility Templates® (VPAT™) documents. Contractor uses the Voluntary Product Accessibility Template (VPAT) to report how products conform to Section 508 standards (Section 508 of the Rehabilitation Act of 1973, amended in 1998). VPAT Reports and additional WCAG Reports can be provided upon request.

60. RIGHT TO AUDIT: Right to Audit shall be as outlined in the NASPO ValuePoint Master Agreement AR3228 Attachment A Section 29.

61. LARGE VOLUME DISCOUNT PRICING: Eligible Users may seek to obtain additional volume discount pricing for large orders provided Contractor is willing to offer additional discounts for large volume orders. No amendment to this Contract is necessary for Contractor to offer discount pricing to an Eligible User for large volume purchases.

62. ELIGIBLE USER PARTICIPATION: Participation under this Contract by Eligible Users is voluntarily determined by each Eligible User. Contractor agrees to supply each Eligible User with Goods based upon the same terms, conditions and prices of this Contract.

63. INDIVIDUAL CUSTOMERS: Each Eligible User that purchases Goods from this Contract will be treated as if they were individual customers. Each Eligible User will be responsible to follow the terms and conditions of this Contract. Contractor agrees that each Eligible User will be responsible for their own charges, fees, and liabilities. Contractor shall apply the charges to each Eligible User individually. The Division is not responsible for any unpaid invoice.

64. QUANTITY ESTIMATES: The Division does not guarantee any purchase amount under this Contract. Estimated quantities are for Solicitation purposes only and are not to be construed as a guarantee.

65. ORDERING: Orders will be placed by the using Eligible User directly with Contractor. All orders will be shipped promptly in accordance with the terms of this Contract.

66. REPORTS AND FEES:

1. **Administrative Fee:** Contractor agrees to provide a quarterly administrative fee to the State in the form of a check,EFT or online payment through the Division's Automated Vendor Usage Management System. Checks will be payable to the "State of Utah Division of Purchasing" and will be sent to State of Utah, Division of Purchasing, 3150 State Office Building, Capitol Hill, PO Box 141061, Salt Lake City, UT 84114. The Administrative Fee will be one quarter of one percent (or 0.25%) and will apply to all purchases (net of any returns, credits, or adjustments) made under this Contract.

2. **Quarterly Reports:** Contractor agrees to provide a quarterly utilization report, reflecting net sales to the State during the associated fee period. The report will show the dollar volume of purchases by each Eligible User. The quarterly report will be provided in secure electronic format through the Division's Automated Vendor Usage Management System found at: https://statecontracts.utah.gov/Vendor.

3. **Report Schedule:** Quarterly utilization reports shall be made in accordance with the following schedule:

Period End	Reports Due
March 31	April 30
June 30	July 31
September 30	October 31
December 31	January 31

4. **Fee Payment:** After the Division receives the quarterly utilization report it will send Contractor an invoice for the total quarterly administrative fee owed to the Division. Contractor shall pay the quarterly administrative fee within thirty (30) days from receipt of invoice.

5. **Timely Reports and Fees:** If the quarterly administrative fee is not paid by thirty (30) days of receipt of invoice or quarterly utilization reports are not received by the report due date, then Contractor will be in material breach of this Contract.

If Services are applicable to this Contract, the following terms and conditions apply to this Contract:

67. TIME IS OF THE ESSENCE: Contractor will provide Services as specified in an accepted Order, and will use all commercially reasonable efforts to deliver in the agreed upon deadline stated in the Order.

68. PERFORMANCE EVALUATION: The Division may conduct a performance evaluation of Contractor's Services, including Contractor's Subcontractors, if any. Results of any evaluation may be made available to the Contractor upon Contractor's request.

69. ADDITIONAL INSURANCE REQUIREMENTS:

1. Professional liability insurance in the amount as described in the Solicitation for this Contract, if applicable.

2. Any other insurance policies described or referenced in the Solicitation for this Contract.

3. Any type of insurance or any increase of limits of liability not described in this Contract which the Contractor requires for its own protection or on account of any federal, state, or local statute, rule, or regulation shall be its own responsibility, and shall be provided at Contractor's own expense.

4. The carrying of insurance required by this Contract shall not be interpreted as relieving the Contractor of any other responsibility or liability under this Contract or any applicable law, statute, rule, regulation, or order. Contractor must provide proof of the above listed policies within thirty (30) days of being awarded this Contract.

70. STANDARD OF CARE: The Services of Contractor and its Subcontractors shall be performed in accordance with the standard of care exercised by licensed members of their respective professions having substantial experience providing similar services which similarities include the type, magnitude, and complexity of the Services that are the subject of this Contract.

71. STATE REVIEWS, LIMITATIONS: The Division reserves the right to perform plan checks, plan reviews, other reviews, and/or comment upon the Services of Contractor.

72. TRAVEL COSTS: The following will apply unless otherwise agreed to in the contract: All travel costs associated with the delivery of Services under this Contract will be paid according to the rules and per diem rates found in the Utah Administrative Code R25-7. Invoices containing travel costs outside of these rates will be returned to the Contractor for correction.

8. Subcontractors: Contractor and Fulfillment Partners authorized in the State of *Utah*, as shown on the dedicated Contractor (cooperative contract) website, are approved to provide sales and service support to participants under this Addendum to the NASPO ValuePoint Master Agreement. The Fulfillment Partners participation will be in accordance with the terms and conditions set forth in the aforementioned Master Agreement.

9. Orders: Any order placed by a Participating Entity or Purchasing Entity for a product and/or service available from this Master Agreement shall be deemed to be a sale under (and governed by the prices and other terms and conditions) of the Master Agreement unless the parties to the order agree in writing that another contract or agreement applies to such order.

IN WITNESS, WHEREOF, the parties have executed this Addendum as of the date of execution by both parties below.

Participating Entity:	Contractor:
State of Utah Division of Purchasing & General Services	Hewlett Packard Enterprise Company
Signature: 	Signature: 
Name: Christopher Hughes	Name: Chris Backs
Title: Chief Procurement Officer	Title: Sr. Contract Negotiator
Date: Nov 13, 2019	Date: Nov 13, 2019

For questions on executing a participating addendum, please contact:

NASPO ValuePoint: info@naspovaluepoint.org

Hewlett Packard Enterprise

HPE Data Privacy and Security Attachment

This Data Privacy and Security Attachment ("DPSA") governs the privacy and security of Personal Data by HPE in connection with the services described in a transaction document that references this DPSA ("Services") and is made a part of the agreement applicable to the Services between HPE and Customer ("Agreement").

1. This DPSA forms part of the Agreement. To the extent there are any conflicts between the terms of this DPSA and the Agreement, the DPSA shall prevail.
2. Definitions:
   - 2.1. "Business Contact Data" means contact information of Customer's representatives for invoicing, billing, and other business inquiries, (ii) information on Customer's usage of Services, and (iii) other information that HPE collects and needs to communicate with Customer.
   - 2.2. "Controller" means the natural or legal person, public authority, agency, or any other body which alone or jointly with others determines the purposes and means of the Processing of Personal Data in accordance with applicable Privacy Law.
   - 2.3. "Personal Data" or "Customer Personal Data" means any (Customer) information relating to an identified or identifiable natural persons or as otherwise defined in applicable Privacy Laws.
   - 2.4. "Privacy Laws" mean all applicable laws and regulations relating to the Processing of Personal Data and privacy that may exist in the relevant jurisdictions.
   - 2.5. "Process," "Processing," or "Processed" means an operation or set of operations performed on or with Personal Data whether or not by automatic means (including, without limitation, accessing, collecting, recording, organizing, retaining, storing, adapting or altering, retrieving, consulting, using, disclosing, making available, aligning, combining, blocking, erasing, and destroying Personal Data) and any equivalent definitions in Privacy Law to the extent that such definition should modify this definition.
   - 2.6. "Processor" means any natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of a Controller or on the instruction of another Processor acting on behalf of a Controller.
3. Appointment and Instructions:
   - 3.1. HPE shall Process Customer Personal Data as necessary to provide the Services and to meet HPE's obligations under this DPSA, the Agreement, and applicable Privacy Law as a service provider and Processor of Customer Personal Data. Details of the Processing, including the subject matter, purpose, and duration of the Processing, the types of Personal Data, and the categories of data are set out in the applicable transaction document.
   - 3.2. HPE shall Process Customer Personal Data in accordance with Customer's instructions as set out in this DPSA, the Agreement, or other documented instructions between HPE and Customer. Potential costs and charges associated with such additional instructions shall be agreed pursuant to the terms of the Agreement.
   - 3.3. HPE may Process Customer Personal Data other than on the instructions of Customer if it is required under law applicable to HPE. In this situation, HPE shall inform Customer of such a requirement before HPE Processes Customer Personal Data unless the law prohibits this on important grounds of public interest. If HPE is unable to comply with Customer's instructions or this DPSA due to changes in legislation or, if HPE believes (without having to conduct a comprehensive legal analysis) that any instruction from Customer will violate applicable law or for any other reason, HPE shall promptly notify Customer in writing.
   - 3.4. HPE acknowledges that HPE has no right, title, or interest in Customer Personal Data (including all intellectual property or proprietary information contained therein). HPE may not sell, rent, or lease Customer Personal Data to anyone.
   - 3.5. If Customer uses the Services to Process any categories of data not expressly covered by this DPSA, Customer acts at its own risk and HPE shall not be responsible for any potential compliance deficits related to such use.

Hewlett Packard Enterprise

4. Compliance with laws

4.1. The Parties shall at all times comply with their respective obligations under this DPSA and Privacy Laws that apply to their respective processing of Personal Data. In addition, if HPE interacts with Protected Health Information as defined under the Health Insurance Privacy and Portability Act, the parties agree to comply with the terms of the Business Associate Agreement found at www.hpe.com/info/customer-privacy.html.

4.2. HPE shall also comply with all applicable laws and HPE's privacy policy with respect to the Processing of Business Contact Data and use Business Contact Data only for legitimate business purposes, including, without limitation, invoicing, collections, service usage monitoring and optimization, service improvements, maintenance, support, communications relating to contract renewals (directly or through a subprocessor acting on HPE's behalf or an HPE approved reseller for contract renewal purposes), and information about new and additional services.

4.3. Where HPE discloses its personnel's personal data to Customer or HPE personnel provide their personal data directly to Customer, which Customer Processes to manage its use of the Services, Customer shall Process that data in accordance with its privacy policies and applicable Privacy Laws. Such disclosures shall be made by HPE only where lawful for the purposes of contract management, service management, or Customer's reasonable and lawful background screening verification or security purposes.

5. Security

5.1. HPE shall implement and maintain the physical, technical, and organizational security measures set out in the applicable transaction document, to protect Customer Personal Data and Business Contact Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure, or access.

5.2. Customer acknowledges that HPE may change the security measures through the adoption of new or enhanced security technologies and authorises HPE to make such changes provided that they do not diminish the level of protection. HPE shall make information about the most up to date security measures applicable to the Services available to Customer upon request.

5.3. Computers and servers have reasonable up-to-date versions of system security software which may include host firewall, anti-virus protection, and up-to-date patches and virus definitions. Software is configured to scan for and promptly remove or fix identified findings. HPE maintains logs of various components of the infrastructure and an intrusion detection system to monitor, detect, and report misuse patterns, suspicious activities, unauthorized users, and other actual and threatened security risks.

5.4. Employees and contractors are trained on HPE's privacy and security policies and made aware of their responsibilities with regard to privacy and security practices. HPE employees and contractors are contractually bound to maintain the confidence of Customer Personal Data and comply with applicable HPE policies, standards, or requirements in relation to the Processing of Customer Personal Data. Failure to comply with those policies, standards, or requirements will be subject to investigation which may result in disciplinary action up to and including termination of employment or engagement by HPE.

5.5. In the event HPE confirms a security breach leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, Customer Personal Data ("Security Incident"), HPE will:

5.5.1. without undue delay, notify Customer of the Security Incident. HPE will provide Customer with updates on the status of the Security Incident until the matter has been remediated. The reports will include, without limitation, a description of the Security Incident, actions taken, and remediation plans. If Customer becomes aware of a Security Incident that affects the Services, Customer shall promptly notify HPE of such and inform HPE of the scope of the Security Incident. Notice shall be provided to HPE Security Operations Center via email at soc@hpe.com and/or to 1-877-762-6139.

5.5.2. at the request and cost of the Customer, (i) provide reasonable assistance to the Customer in notifying a security breach to the supervisory authority competent under the Privacy Laws applicable to the Customer; and (ii) provide reasonable assistance to the Customer in communicating a data breach to data subjects in cases where the data breach is likely to result in a high risk to the rights and freedoms of individuals.

6. Subprocessing and Location of Processing

6.1. Customer authorises HPE to engage affiliated and unaffiliated subprocessors ("Subprocessors") to perform some or all of its obligations under the Agreement. Only where necessary to provide the Services, HPE will provide its Subprocessors with access to Customer Personal Data.

6.2. The Subprocessors applicable to the Services and location of processing can be found at www.hpe.com/info/customer-privacy.html and are deemed as approved by Customer. Customer will subscribe to HPE's notification tool on the above website, and in the event of changes to approved Subprocessors, HPE will notify Customer via the notice subscription tool. Customer shall have ten (10) business days from receipt of the information on Subprocessors to object to the appointment or replacement of a Subprocessor, and the parties shall use all reasonable endeavours to resolve Customer's objection. If the parties fail to resolve Customer's objection within a reasonable period of time, the matter shall be addressed pursuant to the dispute resolution procedure in the Agreement. In case HPE and customer fail to agree on an amicable resolution to the proposed subprocessor change, HPE shall have a right to terminate the contract without further obligations.

6.3. HPE shall conduct appropriate due diligence of its Subprocessors and execute valid, enforceable, and written contracts with Subprocessors requiring the Subprocessor to abide by terms no less protective than those in this DPSA regarding the Processing and protection of Customer Personal Data (including the EU Model Contract terms relating to data importers in the case of an onward transfer of EU, EEA, or Swiss Personal Data to a non-adequate country).

6.4. HPE remains responsible for the acts and omissions of the affiliates and Subprocessors it engages to provide the Services to Customers giving rise to a breach of this DPSA as if they were its own acts or omissions.

7. Audit and Assurance

7.1. Customer shall have the right to conduct additional audits of HPE's compliance with its obligations under this DPSA in accordance with the Agreement. The audit rights are generally exercised in consultation with HPE. HPE is obliged to assist Customer in such audits and any audits of the competent authorities. These audits must be carried out in consideration of the business processes and HPE's need for security and confidentiality.

7.2. Certain information about HPE's security standards and practices are sensitive confidential information which will not be disclosed by HPE to Customer. Upon request, HPE agrees to respond, no more than once per year, to a reasonable information security questionnaire concerning security practices specific to the Services provided hereunder.

7.3. On Customer's request, HPE shall within a reasonable timeframe make appropriate information available to Customer to demonstrate its compliance with applicable Privacy Law, save where that information is readily available to Customer direct through its use of the Services.

8. Providing Customer Assistance

8.1. At Customer's request HPE shall cooperate with Customer and provide Customer with assistance necessary to facilitate the Processing of Customer Personal Data in compliance with Privacy Laws applicable to Customer in relation to HPE Services, including by way of example:

8.1.1. assist Customer by implementing appropriate and reasonable technical and organizational measures, insofar as this is possible, to assist with Customer's obligation to respond to requests from individuals seeking to exercise their rights under the Privacy Laws applicable to Customer;

8.1.2. provide reasonable assistance to Customer in Customer's assessment and implementation of appropriate technical and organizational measures to ensure a level of security appropriate to the risks represented by the Processing and the nature of Customer Personal Data;

8.1.3. the notification of Security Incidents pursuant to section 5.5;

8.1.4. provide reasonable assistance to Customer in carrying out a privacy impact assessment and associated consultations with a supervisory authority for new technologies or products on the protection of Customer Personal Data.

8.2. If Customer requests cooperation or assistance pursuant to this Section, Customer shall notify HPE in writing of the requirements and formulate Customer's instructions. HPE shall respond within a reasonable period of time and provide Customer with approximate time and fee estimates for the implementation of any changes necessary to accommodate Customer's compliance needs. To the extent that compliance with this Section constitutes a change to the scope of the Services, the parties shall, acting reasonably, agree on appropriate change order.

9. Data Quality, Retrieval and Destruction, Repair, or Replacement Service

9.1. To the extent that Customer is not able to access Customer Personal Data itself, HPE shall on Customer's written request (i) update, correct, or delete Customer Personal Data; and/or (ii) provide copies of Customer Personal Data.

9.2. Upon termination of the Agreement, HPE shall at the election of Customer return or delete Customer Personal Data and HPE shall not retain copies of Customer Personal Data unless otherwise agreed with Customer or where it is required to do so under applicable law, in which case HPE shall stop actively Processing the data and maintain the security and confidentiality of the data.

9.3. With regard to the repair or replacement of data carriers (server, hard-disks, SSD, flash-disks, memory etc.), Customer will either purchase the optional (C)DMR Service or adequately wipe (following the NIST Standard) carriers prior to providing them to HPE.

10. Data Transfers

10.1. To address the transfer of EU, EEA, or Swiss Personal Data by Customer or a Customer affiliate to HPE or an HPE affiliate located in a country which is not approved by the European Commission as providing adequate protection for personal data pursuant to Article 45(3) of the General Data Protection Regulation, the execution of a controller to processor EU Model Contract ("EU Model Contract") is required in connection with the Services. Customer hereby authorizes HPE to execute an EU Model Contract on its and its affiliates' behalf.

10.2. When interpreting the EU Model Contract, the term "Member State in which the data exporter is established" will be interpreted to mean (as appropriate) Switzerland or the EU or EEA member state in which the Data Exporter (as defined in the EU Model Contract) is established.

10.3. In the case of any conflict between the EU Model Contract, the terms of this DPSA, and the Agreement, to the extent HPE Processes the Personal Data of EEA or Swiss residents, the EU Model Contract shall prevail but only to the extent necessary to resolve the conflict or inconsistency.

10.4. Any audit pursuant to an EU Model Contract shall be conducted in accordance with the general procedures for audits provided in the Agreement except to the extent expressly required by a regulatory authority or Privacy Laws. Customer shall use commercially reasonable efforts to notify the regulatory authority of the audit requirements of the Agreement and to request that the audit be conducted in accordance with those requirements.

10.5. Any losses suffered by the parties or their respective affiliates under the EU Model Contract shall be treated as if they had been suffered by Customer or HPE respectively and shall in all cases be recovered by Customer or HPE subject to any limits on that party's liability in the Agreement. Nothing in this Section shall limit the liability of either party in relation to a claim by a data subject under an EU Model Contract.

10.6. In the event that EU Model Contracts are no longer a valid transfer mechanism or where HPE commits to an alternative valid transfer mechanism (e.g. Binding Corporate Rules for Processors), HPE shall notify Customer of the mechanism and seek Customer's agreement to rely on this mechanism instead of the EU Model Contract.