February 10, 2022

REQUEST FOR PROPOSAL "RFP" No. PS20210159
CONSULTING SERVICES FOR SAP S/4HANA CONVERSION

ADDENDUM No. 1

RE: PART B – CITY REQUIREMENTS

PLEASE ADD:

9.0 ADDITIONAL REQURIEMENTS

9.1 Privacy Requirement

1) Some personnel from the Successful Proponent will have access to personal data as part of the engagement including but not limited to the data in the Human Capital Management Module.

2) The Successful Proponent must protect all personal information (defined as all recorded information about an identifiable individual, in compliance with the Freedon of Information and Protection of Privacy Act (British Columbia) "FOIPPA"). These responsibilities are outlined in the *Appendix E - Privacy Compliance and Data Security* of Part D – Form of Agreement.

9.2 Vancouver Police Department ("VPD") Enhanced Security Clearance

1) The City's Positions of Trust Policy requires that contractors as well as employees with access to personal information maintain a VPD Enhanced Security Clearance. This is similar to programs run by Federal government and Royal Canadian Mounted Police ("RCMP"). The City will only accept team members with this clearance for these roles.

2) The Successful Proponent is responsible for obtaining this clearance and bearing any and all costs associated with this clearance requirement. Standard fees are approximately $650 per person, and the process takes a minimum of 2 weeks (it may take significantly longer for those not resident in Canada). The City will provide the forms to start the process.

City of Vancouver, Finance, Risk and Supply Chain Management
453 West 12th Avenue
Vancouver, British Columbia V5Y 1V4 Canada
tel: 604.873.7263 *fax:* 604.873.7057
website: vancouver.ca

RE: PART C – FORM OF PROPOSAL, APPENDIX 2 – QUESTIONNAIRE, SECTION 4.0 SCOPE & REQUIREMENTS

PLEASE ADD:

Reference	Requirement
4.10	Confirm whether your organization, if awarded, is able to meet the City's requirements stated in RFP Part B Section 9.1 – Privacy Requirement. Please identify areas of concern (if any).
Response	
4.11	Confirm whether your organization is able to to meet the City's requirements stated in RFP Part B Section 9.2 – VPD Enhanced Security Clearance. (Yes or No) If yes, provide details about:- • Which team members will need this clearance? • Will any of these staff be working physically outside of Canada? If yes, please state where they will be working?
Response	
4.12	When evaluating, the City will consider risk factors e.g. cyber security, knowledge transfer, communication. Provide details about team members working outside of Canada, including • Where will they be located? • What special skills do they provide and what will they be working on? • How risks associated with the location will be mitigaged?
Response	

RE: PART D – FORM OF AGREEMENT

PLEASE ADD:

APPENDIX E - PRIVACY COMPLIANCE AND DATA SECURITY

Certain terms used in this document will have the meanings given below or in the Agreement. Vendor shall comply with the following terms and conditions relating to data security and compliance with applicable privacy legislation in respect of any personal information (as defined in section 1.1 below) acquired or accessed by Vendor in connection with the Agreement.

1.0 GENERAL

1.1 The following terms used in this document will have the following meanings:

(a) **"FOIPPA"** means the Freedom *of Information and Protection of Privacy Act* (British Columbia) as it may be amended or superseded from time to time;

(b) "**personal information**" has the meaning given in FOIPPA, PIPA or PIPEDA as applicable;

(c) **"PIPA"** means the *Personal* Information *Protection Act* (British Columbia) as it may be amended or superseded from time to time;

(d) **"PIPEDA"** means the Personal *Information Protection and Electronic Documents Act* (Canada) as it may be amended or superseded from time to time; and

(e) "**Transmitted Data**" means all data or information acquired, accessed or sent by the Vendor as a result of this Agreement, including all data or information acquired, accessed or sent by or through any software used by the Vendor to perform services under this Agreement, which data may include, without limitation, personal information and City proprietary or confidential information.

1.2 The Vendor shall not assign any of its rights or obligations under this document to a third party without the prior written consent of the City. If the City consents to the Vendor assigning certain of its rights or obligations to a third party, in addition to any other conditions the City may require, the Vendor shall ensure, and shall cause, its assignee to comply with the privacy and data security obligations set out in this document. Alternatively, in respect of complying with data security obligations hereunder, if the City consents to the Vendor using a third party to store the Transmitted Data (e.g. if the Vendor elects to use Infrastructure as a Service (Iaas) or Platform as a Service (Paas)), evidence satisfactory to the City that such third party is able to substantially comply with similar or a higher standard of data security than as set out in this document (e.g. ISO27001 SOC 2 Type II) shall be provided by the Vendor to the City.

2.0 PRIVACY AND DATA SECURITY

2.1 **Acknowledgment:** Vendor acknowledges that under this Agreement, it will acquire or have access to personal information. Vendor further acknowledges that both the City and Vendor have obligations under FOIPPA to protect such information and that any unauthorized collection, disclosure, use or storage of such information could result in irreparable and significant harm to the City.

2.2 **Privacy Legislation and Obligations**

(a) the City is subject to the provisions of FOIPPA which imposes significant obligations on the City and its contractors (including Vendor) to protect all personal information acquired, accessed or sent as a result of this Agreement. Vendor confirms and acknowledges its obligations to comply with the provisions of FOIPPA. Vendor further confirms and acknowledges its obligations to comply with all other Applicable Laws relating to privacy and personal information including PIPA and PIPEDA in relation to any personal information (as defined in such statutes) to which Vendor has access under this Agreement.

(b) Vendor has implemented appropriate or will implement appropriate policies and security measures to comply with all Applicable Laws relating to privacy and personal information including FOIPPA, PIPA and PIPEDA, as well as to comply with the terms of this Agreement.

(c) Vendor agrees that all personal information and Transmitted Data to which Vendor has access under this Agreement is "under the control" of the City for the purposes of FOIPPA. The City is only transferring physical custody of such information to Vendor, not control of that information, and the authority over the collection, use, disclosure, access, retention, destruction and integrity of all such information remains with the City. At any time during the term of the Agreement, the City may exercise the foregoing control over any such information by notice in writing to Vendor and Vendor shall comply with the instructions in the City's notice.

(d) Vendor agrees to collect, acquire, or hold only the minimum amount of personal information and Transmitted Data required to perform its duties under this Agreement. Unless otherwise authorized by FOIPPA or other Applicable Law and approved by the City, Vendor must collect personal information directly from the individual to whom the information pertains.

(e) At or prior to the time of collection, Vendor must inform any person from whom it collects personal information:

2.2.e.1 The purpose for collecting it;

2.2.e.2 The legal authority for collecting it;

2.2.e.3 The title, business address and business telephone number of a person who can answer the individual's questions about the collection.

(f) If an access to information request is made to Vendor under Applicable Laws relating to personal information or Transmitted Data to which Vendor has access under this agreement, Vendor shall (i) immediately, and in any event before responding to such information request, notify the City in writing of such request, and (ii) upon the City's request direct such information request to the City for the City to handle. In the case of (ii), Vendor shall, at the City's expense, deliver to the City copies of all relevant information within seven (7) days of notification by the City and shall comply with all other requests of the City.

(g) In the case of an access to information request made to the City, Vendor, at the City's expense, shall deliver to the City copies of all relevant information within seven (7) days of notification by the City and shall comply with all other requests of the City.

(h) All personal information and Transmitted Data shall be treated as confidential and is supplied to Vendor only for the purpose of fulfilling the obligations under this Agreement. This obligation shall survive the expiry or termination of this Agreement. No such information shall be disclosed unless Vendor is legally compelled to do so and having first challenged that requirement and given the City an opportunity to challenge that requirement.

(i) In the event any governmental authorities under applicable privacy laws or otherwise make inquiries to the City or Vendor or take any actions in respect of the personal information or Transmitted Data, Vendor will, upon the City's request, cooperate with such governmental authorities. If such governmental authorities make inquiries or requests of Vendor, Vendor will, to the extent legally required or permitted, give prompt written notice to the City and allow the City to participate in any responses submitted by Vendor to such governmental authorities.

(j) Vendor must provide immediate notification to the City in the event that it receives a foreign demand for disclosure, as defined in s. 30.2 of FOIPPA, or has reason to suspect that unauthorized disclosure of personal information has occurred in response to a foreign demand for disclosure. Notice must include the nature of the foreign demand; who made the foreign demand; when the foreign demand was received; and what information was sought or disclosed in response to the foreign demand.

(k) Once Vendor possesses or has access to personal information and Transmitted Data, such information will be stored and backed-up on servers and other equipment that are owned or controlled by Vendor and that are physically located in Canada. Physical and electronic access to Vendor's servers are locked and restricted to only Vendor employees and authorized agents. If the location of Vendor's primary or back-up servers change, Vendor will promptly notify the City in writing of the address of the new location. Vendor will not store any such information on any other server or equipment without the prior written approval of the City.

(l) Except with the prior written approval of or instructions from the City, Vendor shall not modify, add, delete, destroy, share, sell, match, mine, combine, manipulate or otherwise tamper with the personal information or Transmitted Data in any way.

(m) Vendor shall not withhold any personal information or Transmitted Data to enforce payment by the City or to enforce Vendor's rights in a dispute over this Agreement.

(n) As between the City and Vendor, the personal information and Transmitted Data are owned by the City, Vendor hereby agrees to hold such information in trust for the City, and Vendor makes no claim to any right of ownership in it.

2.3 **Authorized Purposes:** Vendor may only use the personal information and Transmitted Data to which Vendor has access under this Agreement to carry out Vendor's obligations under this Agreement and for no other purpose (**"Authorized Purposes"**). Any use or disclosure of such information by Vendor that is not expressly permitted by this Agreement will require the prior written consent of the City and must comply with all Applicable Laws.

2.4 **Restricted Access**

(a) Vendor will permit access to personal information and Transmitted Data only to those employees and authorized agents who need such access in order to carry out the Authorized Purposes (the **"Authorized Employees"**). Vendor will at all times maintain a current list of Authorized Employees. Vendor will, upon the City's request, provide the City with the list of Authorized Employees.

(b) Vendor will at all times have in place a knowledgeable senior person within its organization to be responsible for, or, to have the authority to ensure, compliance with the terms of this document (the **"Compliance Representative"**). The Compliance Representative will ensure that each Authorized Employee is aware of the terms of this Agreement, and to maintain proof, in writing, that the terms have been explained and understood by each Authorized Employee. Upon entering into this Agreement, Vendor will notify the City in writing as to the name of the Vendor Compliance Representative. Vendor will promptly advise the City of any change to the Compliance Representative.

2.5 **Security:** Vendor will have appropriate physical, organizational and technological security measures (consistent with best practices in the software industry) in place to ensure that all personal information and Transmitted Data is collected, accessed, used, disclosed and destroyed only by Authorized Employees, including without limitation:

(a) restricted access to records containing paper copies of personal information and Transmitted Data;

(b) restricted access to personal information and Transmitted Data stored on computer systems and electronic storage devices and media, by using unique user IDs and passwords that are linked to identifiable Authorized Employees; and

(c) systems containing personal information and Transmitted Data will be capable of providing an audit trail and user access logs, which logs will be retained by Vendor during the term of this Agreement and for at least two (2) years following its expiry, termination, or destruction of the personal information and Transmitted Data.

(d) Vendor must ensure that the data centre and servers containing the personal information and Transmitted Data meets the following physical and electronic security requirements:

2.5.d.1 single point of entry;

2.5.d.2 access only to persons on Vendor approved access list;

2.5.d.3 log-in validation;

2.5.d.4 creation of accounts only as verified by Vendor;

2.5.d.5 external or WIFI access to servers via encrypted means; and

2.5.d.6 servers running behind secure firewall.

2.6 **No Storage, Access or Transmission outside Canada; Limited Exception:**

(a) Subject to the exception set out in subsection 2.6(b) below, Vendor will not (i) store personal information or Transmitted Data outside Canada, (ii) access or make accessible personal information or Transmitted Data from outside Canada, or (iii) otherwise permit any personal information or Transmitted Data to leave Canada.

(b) Notwithstanding the above, Vendor is permitted under subsection 33.1(1)(p) of FOIPPA to disclose personal information outside of Canada strictly under the following limited circumstances:

2.6.b.1 such disclosure is necessary for Vendor to install, implement, maintain, repair, trouble shoot, or upgrade an electronic system or equipment that includes an electronic system, or for data recovery being undertaken following failure of an electronic system;

2.6.b.2 such disclosure is limited to temporary access and storage by Vendor or its authorized sub-contractor outside of Canada for the minimum time and to the minimum amount of information necessary for the purpose set out in s. 33.1(1)(p)(i) of FOIPPA;

2.6.b.3 once the purpose of disclosure is fulfilled, all applicable personal information accessed or retained by Vendor or its authorized sub-contractor is irrevocably and permanently destroyed and deleted and all temporary access to that personal information is revoked. If requested by the City, Vendor has certified the foregoing in writing (with the City having a right to audit or verify the foregoing, acting reasonably);

2.6.b.4 all processes and requirements requested by the City in respect of such disclosure (including, without limitation, how such disclosure will be made (e.g.

through a dedicated VPN) , how such information will be accessed, whether such information may only be viewed outside Canada but not retained, etc.) have been complied with by Vendor;

2.6.b.5 Vendor complies with all Applicable Laws outside Canada regarding Vendor's disclosure and handling of such information provided that if there is a conflict between such Applicable Laws outside Canada and Applicable Laws of Canada (including, without limitation, FOIPPA, PIPA and PIPEDA), Vendor shall first comply with Applicable Laws of Canada; and

2.6.b.6 upon request by the City, acting reasonably, Vendor cooperates in good faith in facilitating the audit or verification of Vendor's compliance with the foregoing by the City.

2.7 **Information Retention, Transfer to the City and Destruction:**

(a) **Vendor's Retention, Transfer to the City and Destruction:** Vendor is only permitted to retain personal information, Transmitted Data or any records of such information in any form whatsoever (including without limitation hard copy or electronic formats) during the term of this Agreement and for one year after the end of the term. During this period of time, Vendor shall hold all such information in compliance with the security, privacy and confidentiality requirements of this Agreement. Any personal information that is used by or on behalf of the City to make a decision that directly affects the individual must be retained for at least one year after being used so the affected individual has a reasonable opportunity to obtain access to that personal information. At any time during the term of this Agreement and for a period of one year after the end of the term, Vendor shall, at the City's request, transfer a copy of any such information to the City in a format reasonably requested by the City. Upon the expiry of one year after the end of the term, Vendor will transfer a copy of all such information to the City in a format reasonably requested by the City and then permanently and securely destroy all such information and all records thereof in a manner that is appropriate for the media so all such information or any portion of it cannot be subsequently retrieved, accessed or used by Vendor or any other person. After all such information is transferred to the City and subsequently destroyed, Vendor shall deliver a written notice of confirmation to the City (in form and substance satisfactory to the City).

2.8 **Inspection and Compliance**

(a) During this Agreement and during the period of time that Vendor is permitted by this document to retain personal information and Transmitted Data, the City's authorized representative may, on reasonable notice and during regular business hours, enter Vendor's premises and/or will be given access to Vendor's computer systems to inspect any personal information and Transmitted Data in the possession of Vendor or any of Vendor's information management policies or practices relevant to its compliance with this Agreement.

(b) the City may request Vendor to provide a written certificate confirming Vendor's compliance with all obligations under this document, and if so requested, Vendor will within ten (10) business days either:

2.8.b.1 provide such certificate; or

2.8.b.2 provide a notice of non-compliance in accordance with section 1.9.

(c) Vendor will promptly forward to the City any records that the City may request in order to review whether Vendor is complying with this Agreement.

(d) If requested by the City, acting reasonably, Vendor will appoint an independent, external auditor at the City's expense to review Vendor's information and security practices

under this Agreement. Vendor will provide copies of the results of any such audit to the City within seven (7) days of receiving the auditor's report.

(e) Vendor will promptly and fully comply with any investigation, review, order or ruling of the Office of the Information and Privacy Commissioner (British Columbia) in connection with the personal information and Transmitted Data.

2.9 **Written Notice of Non-Compliance.** Vendor will immediately notify the City in writing of any non-compliance or anticipated non-compliance with this document and will further inform the City of all steps Vendor proposes to take to address and prevent recurrence of such non-compliance or anticipated non-compliance.

2.10 **Survival:** The obligations in this document shall survive the expiration or earlier termination of this Agreement.

3.0 ADDITIONAL TERMS GOVERNING STORAGE AND ACCESS OF INFORMATION

3.1 Vendor shall, in respect of storage of, and access to, personal information and Transmitted Data**:**

(a) take a physical inventory, at least annually, of all records containing such information, to identify any losses;

(b) ensure that records are not removed from storage premises without appropriate written authorization from the City;

(c) use physically secure areas for the storage of records and restrict access to Authorized Employee;

(d) ensure that access to documentation about computer systems that contain such information is restricted to Authorized Employees;

(e) ensure that users of a system or network that processes such information are uniquely identified and that, before a user is given access to the system or such information, their identification is authenticated each time;

(f) implement procedures for identification and authentication, which include:

(i) controls for the issue, change, cancellation and audit-processing of user identifiers and authentication mechanisms;

(ii) ensuring that authentication codes or passwords:

(1) are generated, controlled and distributed so as to maintain the confidentiality and availability of the authentication code;

(2) are known only to the authorized user of the account;

(3) are pseudo-random in nature or vetted through a verification technique designed to counter triviality and repetition;

(4) are no fewer than 6 characters in length;

(5) are one-way encrypted;

(6) are excluded from unprotected automatic log-on processes; and

(7) are changed at irregular and frequent intervals at least semi-annually;

(g) maintain and implement formal procedures for terminated employees who have access to such information, with prompts to ensure revocation or retrieval of identity badges, keys, passwords and access rights;

(h) take reasonable security measures in respect of such information displayed on computer screens or in hardcopy form to prevent viewing or other access by unauthorized persons;

(i) implement automated or manual controls to prevent unauthorized copying, transmission or printing of such information; and

(j) implement control procedures to ensure the integrity of such information being stored, notably its accuracy and completeness.

3.2 Vendor must store personal information and Transmitted Data on agreed-upon media in accordance with prescribed techniques that store such information in a form that only Authorized Employees may access. These techniques may include translating such information into code (encryption) or shrinking or tightly packaging such information into unreadable form (compression).

3.3 Vendor shall store backup copies of personal information and Transmitted Data off-site under conditions which are the same as or better than originals.

3.4 Vendor shall securely segregate personal information and Transmitted Data from information owned by others (including Vendor), including by installing access barriers to prevent information elements from being associated (including compared or linked, based on similar characteristics) with other information, including:

(a) separate storage facilities for such information;

(b) authorization before a person is granted access to computers containing such information; and

(c) entry passwords and the employment of public key encryption/smart card technology where practicable.

3.5 Vendor shall ensure the integrity of personal information and Transmitted Data stored, processed or transmitted through its system or network.

3.6 Vendor shall co-operate with, and assist in, any City investigation of a complaint or concern that personal information or Transmitted Data has been collected, used, handled, disclosed, stored, retained or destroyed contrary to the terms of this Agreement, FOIPPA, PIPA, PIPEDA or any other Applicable Laws.

3.7 As per section 2.8, the City shall be able to access Vendor's premises and other places where Vendor's servers and other equipment are located to recover any or all the City records, personal information and Transmitted Data and for auditing purposes to ensure compliance with the terms of this Agreement.

All other conditions and specifications remain unchanged.

This addendum must be completed, and attached to your Proposal form.

_____

NAME OF VENDOR

_____

SIGNATURE OF AUTHORIZED SIGNATORY

_____

DATE

Wen Shi

Buyer