RONA Data Privacy Addendum: Service Providers

This Data Privacy Addendum ("**Addendum**") forms part of the agreement between RONA inc. ("**RONA**") and the Vendor for the provision of Services to RONA (the "**Agreement"**).

In consideration of the mutual covenants and premises set forth herein, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereby agree as follows:

This Data Privacy Addendum applies to the Collection and Processing of Personal Information by Vendor, a service provider of RONA's, in performing its obligations or exercising its rights under the Agreement or otherwise in providing Services to RONA. This Addendum shall supersede and replace all prior Data Privacy Addendum. All obligations herein are in addition to, not in lieu of, Vendor's obligations under the Agreement; provided, in the event of a conflict, the terms of this Addendum shall prevail over the Agreement.

1. **Definitions.**
   - **a.** "**Business Purpose**" means the use of Personal Information for the business's or Vendor's operational purposes that are reasonably necessary and proportionate to achieve the purpose for which the Personal Information was Collected or Processed or for another purpose that is compatible with the context in which the Personal Information was Collected. It does not include Collecting or Processing the Personal Information for cross-context behavioral targeted advertising or sharing Personal Information to a third party to build a profile about a Data Subject.
   - **b.** "**Collects,**" "**Collected**," or "**Collection**" means buying, renting, gathering, obtaining, receiving, or accessing any Personal Information by any means, either actively or passively, or by observing a person's behavior.
   - **c.** "**Commercial Purpose**" means to advance a person's commercial or economic interests such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction.
   - **d.** "**Confidential Information**" means all non-public information which is disclosed by RONA, its affiliates as defined in the Business Corporations Act, CQLR c S-31.1 and/or its agents ("**RONA Group**"), whether in written, graphic, machine-readable form, or oral form, and include all Personal Information, and any information obtained visually or aurally during any visits to RONA facilities or meetings with RONA. Confidential Information also includes the existence of the Agreement and this Addendum or any working relationship with RONA, as well as any bids or proposals submitted to RONA in connection with any proposed or actual business relationship. "Confidential Information" does not include any information that: (a) is or subsequently becomes publicly available through no fault of Vendor or Vendor's Personnel; (b) is, and can be proven through trustworthy written records to have been: (i) known to Vendor prior to RONA disclosure of such information to Vendor; (ii) received by Vendor from a third party who obtained such information without restrictions and without any obligation of confidentiality to RONA; or (iii) independently developed by Vendor; or (c) is approved for release by written authorization from an officer of RONA. Failure to mark any "Confidential Information" as confidential will not affect its status as Confidential Information under the Agreement and this Addendum.
   - **e.** "**Data Protection Law**" means all applicable data protection or privacy conventions, treaties, common law, statutes, codes, laws, regulations, rules, judgments, orders, ordinances, and mandates, including, without limitation, the *Act Respecting the Protection of Personal Information in the Private Sector* P-39.1 or any federal, provincial, or state law equivalent each as they may be amended or otherwise updated from time to time.
   - **f.** "**Data Subject**" means the identified or identifiable person to whom the Personal Information directly or indirectly relates.
   - **g.** "**Data Subject Request**" means a request from a Data Subject to exercise a potential right under Data Protection Law, such as a request to access, correct, delete, cease dissemination, de-index, re-index or transfer Personal Information.
   - **h.** "**Deidentified Data**" means data created using Personal Information that cannot reasonably be linked to such Personal Information, directly or indirectly.
   - **i.** "**Deliverables**" means any and all information, works, drawings, documents, designs, specifications, graphics, data, inventions, discoveries, improvements, works of authorship, creative works, ideas, knowledge, know-how, content, and other tangible and intangible materials, in whatever form and whether existing singularly or in combination with other materials, which are authored, prepared, created, delivered or

developed, solely or collaboratively with others, by Vendor in connection with the performance of its obligations under or in anticipation of the Agreement and this Addendum.

j. "**Permitted Purpose**" means solely for the specific Business Purpose of performing the Services specified in the Agreement. Permitted Purpose does not include any Commercial Purpose other than the Business Purposes specified in the Agreement unless otherwise permitted by applicable Data Protection Laws.

k. **"Personal Information**" means any information Processed by Vendor on behalf of RONA that: (i) directly or indirectly identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to a particular Data Subject; or (ii) is otherwise deemed "personal information" or "personal data" under Data Protection Law. Personal Information shall, at all times, constitute and be treated as "Confidential Information" (as defined in the Agreement) whether or not it meets the definition of Confidential Information under the Agreement and/or is subject to an exclusion from such definition or obligations.

l. **"Process"** or **"Processing"** means any operation or set of operations that are performed on Personal Information or on sets of Personal Information, whether or not by automated means, such as Collection, use, storage, or communication.

m. "**Security Breach**" means any actual or suspected unauthorized access to or use, disclosure, alteration, or destruction of Confidential Information, or any act or omission that compromises the physical, technical, administrative or organizational safeguards put in place by Vendor that relate to the protection of the security, confidentiality or integrity of Confidential Information.

n. "**Sell**" and "**Sold"** means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's Personal Information by the business to a third party for monetary or other valuable consideration or has otherwise defined under applicable Data Protection Laws.

o. "**Share**" has the meaning sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's Personal Information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged or has otherwise defined under applicable Data Protection Laws.

2. Processing and Collection of Personal Information.

a. Roles of the Parties. The parties acknowledge and agree that (i) RONA determines the purposes and means of Vendor's Collection and Processing of Personal Information; and (ii) Vendor Collects Personal Information on RONA behalf pursuant to the Agreement for the Permitted Purpose.

b. Permitted Purpose. The Parties acknowledge and agree that this Addendum and the Agreement include the nature and purpose of the Processing, the type of Personal Information subject to the Processing, the duration of the Processing, and the rights and obligations of both Parties. Vendor shall not, unless expressly permitted by applicable Data Protection Laws, (i) retain, use or disclose the Personal Information Collected pursuant the Agreement outside of the direct business relationship between RONA and Vendor; (ii) Process the Personal Information Collected Pursuant to the Agreement for any purpose other than the Permitted Purpose specified in the Agreement or as otherwise permitted by Data Protection Law; (iii) Sell or Share the Personal Information or otherwise make the Personal Information available to any third party for monetary or other valuable consideration.

c. Compliance. Each party shall comply with its obligations pursuant to Data Protection Law, this Addendum, and the Agreement when Collecting or Processing Personal Information. Vendor shall provide the same level of privacy protections as required of RONA by the applicable Data Protection Laws. Vendor shall notify RONA promptly if Vendor determines that it can no longer meet its obligations under Data Protection Law. RONA will have the right to take reasonable and appropriate steps to stop and remediate unauthorized Personal Information use upon providing reasonable notification. Vendor undertakes to implement any reasonable mitigation or control measures recommended by RONA in accordance with Data Protection Laws. Vendor shall provide documentation demonstrating its compliance with applicable Data Protection Law upon RONA reasonable request.

d. Security Breach.

a. In the event that Vendor becomes aware of any Security Breach of Confidential Information (including Personal Information), Vendor will immediately notify RONA of such Security Breach, even if the details of the Security Breach have not been fully confirmed. Notwithstanding the "Notices" Section, all Security Breach notifications will be made via email to SOC@RONA.ca, dataprivacy@RONA.ca and by phone to 1-877-599-5900 ext. 6059. Vendor will, at its own expense, diligently work to determine the nature, cause, and extent of any Security Breach, and will: (i) perform a root cause analysis thereon; (ii) investigate such Security Breach and report its findings to RONA; (iii) provide RONA with a remediation plan, acceptable to RONA, to address the Security Breach and prevent any further incidents; (iv) remediate such Security Breach in accordance with such approved plan; (v) conduct a forensic investigation to determine what systems, data and information have been affected by such event; and (vi) cooperate with RONA in execution of its security incident response plan and otherwise, including, at RONA request, cooperation with any law enforcement or regulatory officials, credit reporting companies, and credit card associations investigating such Security Breach. Vendor will provide RONA with a primary contact who will be available to RONA 24 hours a day, seven days a week to assist in resolving obligations associated with a Security Breach. Without limiting the foregoing, and notwithstanding anything herein to the contrary, RONA will make the final decision on notifying any third party of the Security Breach, and the implementation of the remediation plan.

b. If, in RONA commercially reasonable judgment, a Security Breach notification to a customer, employee, or other person and/or a report to relevant regulatory officials are required under any Law or pursuant to RONA privacy or security policies, then notifications to all customers, employees, or other persons who are affected by the same event (as reasonably determined by RONA) and reports to relevant regulatory officials will be considered legally required. Vendor will reimburse RONA on demand for all reasonable Notification Related Costs incurred by RONA arising out of or in connection with any such Security Breach resulting in legally required notifications and reports (as determined in accordance with the previous sentence).

e. Data Subject Request Assistance. Vendor agrees to reasonably cooperate and comply with any request made by RONA to Vendor to assist RONA in complying with Data Subject Requests under Data Protection Law. Vendor shall complete its cooperation and compliance with RONA request within a reasonable time that allows RONA to satisfy its obligations under the applicable Data Protection Laws. Vendor shall maintain a single point of contact for privacy-related inquiries or notifications from RONA. Vendor is responsible for updating contact information by emailing dataprivacy@rona.ca.

f. Inquiries and Requests. In the event that any Data Subject Request or other request, correspondence, inquiry, or complaint from a Data Subject, regulatory authority, or any person is made directly to Vendor in connection with Vendor's Processing of Personal Information, Vendor shall promptly – but no later than within two (2) business days upon its reception – (i) inform RONA at dataprivacy@rona.ca and provide details of the same, to the extent legally permitted; or (ii) if such request is from a Data Subject and relating to Personal Information Processed in connection with RONA Services, direct the individual to the RONA online privacy portal. Unless legally obligated to do so, Vendor shall not respond to any such request, inquiry, or complaint without RONA prior consent except to confirm the request relates to RONA. Nothing herein shall limit Vendor's legal obligations to respond directly to such requests, inquiries, or complaints.

g. Privacy Contacts. Vendor shall maintain a single point of contact for privacy-related inquiries or notifications from RONA ("**Privacy Contact**"). Vendor is responsible for updating contact information by dataprivacy@rona.ca.

h. Data Disposition. Upon completion of the services under the Agreement, Vendor shall, at RONA option and request, (i) return or destroy the Processing of Personal Information; and (ii) delete and procure the deletion of all other copies of Personal Information Processed by Vendor or any subcontractors.

i. Subcontractor. Unless otherwise provided under the Agreement, Vendor shall not disclose Personal Information to any third party or permit a third party to Process Personal Information without RONA prior

written consent. If permitted to subcontract, Vendor shall enter into a written agreement incorporating terms which are substantially similar to those set out in this Addendum. Vendor shall also ensure that each subcontractor or any person it authorizes to Process Personal Information shall protect the Personal Information in accordance with Vendor's obligations under this Addendum and the Agreement. Vendor shall remain fully liable for all acts or omissions of any third parties or authorized persons that violate or otherwise do not comply with the obligations under this Addendum and the Agreement as if they were the acts and omissions of Vendor. Vendor will limit access to Personal Information to personnel who have a business need to have access to such Personal Information.

j. Deidentified Data. If Vendor receives Deidentified Data from or on behalf of RONA, then Vendor will: (i) take reasonable measures to ensure the information cannot be associated with a Data Subject; (ii) commit to Process the Deidentified Data solely in deidentified from and not to attempt to reidentify the information; (iii) contractually obligate any recipients of the Deidentified Data to comply with the foregoing requirements and Data Protection Law.

k. Compliance Assessments. RONA has the right to take reasonable and appropriate steps to ensure that Vendor uses Personal Information in a manner consistent with RONA obligations under Data Protection Law. RONA may conduct any compliance review itself or engage an independent third-party auditor to conduct the review on RONA behalf, subject to a reasonable confidentiality commitment to Vendor. Compliance review may be performed no more than once annually, unless there are indications of noncompliance with applicable Data Protection Law or material non-compliance with this DPA, in which case: (i) more frequent follow-up reviews will be permitted to confirm that the non-compliance has been remedied; and (ii) Vendor will be responsible for RONA reasonable review costs with regard to the audit that identified the non-compliance and related follow-up audits. Vendor will provide RONA with information to enable RONA to conduct and document any data protection assessments required under Data Protection Law. Without limiting the foregoing, if the Personal Information will be transferred internationally in a manner that requires a risk assessment under Data Protection Law, then the Parties will evaluate applicable risks and work in good faith to implement supplementary measures to provide adequate protection for Personal Information under Data Protection Law.

l. Security.

a. During the Term of this Agreement and this Addendum, and thereafter, Vendor will maintain all Confidential and Personal Information in confidence, and will not, except as otherwise permitted herein or directed in writing by RONA, use, copy, reproduce, or remanufacture, or disclose or permit any unauthorized person access to, any Personal or Confidential Information, whether learned by or disclosed to Vendor before or after the Effective Date and irrespective of the form of communication. Vendor will limit access to Confidential and Personal Information to only its counsel, officers, and employees reasonably needing to know the Confidential Information and Personal Information in order to conduct business with RONA and then only on the following conditions: (i) each authorized employee to whom Confidential or Personal Information is communicated will be informed of the Agreement and this Addendum and that the Confidential and Personal Information is confidential hereunder; and (ii) prior to receiving any Confidential or Personal Information, each authorized employee of Vendor will be informed not to use Confidential or Personal Information except for the purpose of conducting business with RONA, to RONA benefit and as otherwise permitted by RONA. Notwithstanding the provisions of this section, Vendor may disclose Confidential or Personal Information to the extent that Confidential or Personal Information is required to be disclosed pursuant to a requirement of a governmental agency or Law, provided that: (i) Vendor has given RONA prior written notice of such disclosure and takes all available steps to maintain the confidentiality of the information disclosed; and (ii) RONA has been afforded a reasonable opportunity to contest the necessity, scope and/or conditions of such disclosure.

b. All software, computer disks, technical information, data records, files, memoranda, reports, price lists, customer lists, drawings, plans, sketches, notes, documents and the like (together with all copies and all computer files stored in any medium thereof) relating to the business of RONA, and all materials provided by RONA in any form, format or medium (including computer files stored in any

medium), which Vendor receives, has access to or comes in contact with as a result of, the Agreement, any SOW and this Addendum (collectively, the "Materials") will, as between the parties hereto, remain the sole property of RONA. Subject to Vendor's document retention obligations under the law, upon RONA's request, Vendor will immediately return any Material and delete or destroy all computer files and all copies of the Material in any form, format or medium whatsoever.

c. Vendor will, upon the earlier of RONA request or termination of the Agreement, immediately cease any use and return or destroy all or designated written and/or tangible Confidential or Personal Information. RONA, in its sole discretion, will be entitled to determine whether such written and/or tangible Confidential or Personal Information will be returned or destroyed and the manner of such return or destruction. With respect to the Confidential and Personal Information returned or destroyed, Vendor will not retain any copies or extracts, in whole or in part. Any such return or destruction will be certified by an officer of Vendor supervising the same.

d. Vendor will establish an information security program with respect to Confidential and Personal Information which: (i) ensures the security and confidentiality of Confidential and Personal Information; (ii) protects against reasonably anticipated threats or hazards to the security or integrity of Confidential and Personal Information; and (iii) protects against unauthorized access to, use or transfer of Confidential and Personal Information. Vendor also will establish and maintain network and internet security procedures, protocols, security gateways and firewalls with respect to Confidential and Personal Information. All the foregoing will be consistent with and be no less rigorous than those safeguards and procedures required by Law, or, if more stringent than required by Law, those maintained by RONA for such data prior to the date on which the Confidential Information is provided to or collected by Vendor, if any. In no event will such protections be less rigorous than those maintained by Vendor for its own data and information of a similar nature. Vendor will maintain a data compromise incident response plan that contains, at a minimum, the following: (i) roles, responsibilities, and communication strategies in the event of a compromise; (ii) specific incident response procedures; (iii) business recovery and continuity procedures and systems to ensure the security and integrity of Confidential and Personal Information in the event of a disruption, disaster or failure of RONA or Vendor's primary data systems; (iv) data backup processes; (v) analysis of legal requirements for reporting compromises; and (vi) coverage and responses for all critical system components.

e. If applicable, Vendor will physically or logically segregate Personal Information, and will ensure that it does not combine Personal Information with any other data to which Vendor may have access. Vendor will protect Personal Information, while the Personal Information is in transit and at rest, using a form of data encryption, obfuscation, masking, or cloaking which are adequate to the nature of information in transit and approved by RONA.

f. Vendor may only authorize a third party (subcontractor) to process Personal Information if (i) RONA is given an opportunity to object within thirty (30) days after the Vendor supplies RONA with full details regarding such subcontractor; (ii) Vendor enters into a written contract with the subcontractor that contains terms substantially the same as those set out in the Agreement or this Addendum and, upon RONA's written request, provides RONA with copies of such contracts; and (iii) Vendor maintains control over all Personal Information it entrusts to the subcontractor. Furthermore, Vendor will not transfer any Personal Information to another country unless the transfer is carried out in compliance with the applicable law.

g. Vendor recognizes RONA commitment to customer and employee privacy and data security and acknowledges that RONA expects Vendor to fulfill its obligations hereunder in a manner consistent with that commitment. To meet that expectation, Vendor agrees to comply, and to cause its personnel to comply, with: (a) current and future federal, provincial and territorial laws, legislation and industry self-regulation concerning data privacy and data security, to the full extent applicable to RONA and/or Vendor; (b) to the extent applicable to Vendor's performance or provision of services under the Agreement or Deliverables, any privacy policies posted on any public RONA-affiliated website, including those posted on Rona.ca; and (c) the terms of this Addendum.

h. To the greatest extent permitted by Law, Vendor will indemnify, defend and hold harmless RONA Group, their respective officers and employees from and against any and all liabilities, damages, losses, claims, demands (including any subpoenas, civil investigative demands, or other compulsory processes received by RONA), assessments, actions (including declaratory judgment actions brought by RONA Group, as well as the respective officers, employees, agents, successors and assigns in response to a claim described herein), class actions, causes of action, costs (including reasonable attorneys' fees and expenses) and any of them, arising out of or resulting directly or indirectly from for any Security Breach resulting from Vendor's fault or Vendor's breach of the Agreement or this Addendum. In addition, Vendor will maintain adequate insurance (cyber) coverage for any Security Breach and provide RONA with the insurance police upon RONA's request. As a minimum, the (cyber) insurance will cover civil liability for network security and a minimum limit of $ 5,000,000 by event covering without being limited to, criminal actions of Vendor's employees. RONA, its subsidiaries and related entities will be added as additional insured for Vendor's wrongful acts with an exception to the exclusion "insured versus insured". Such insurance will be maintained during the period of three (3) years after the termination of the Agreement with a retroactive date prior to the date of signature.

i. Vendor will use commercially reasonable measures to screen any software or electronic data or other products provided or made available by it to RONA to avoid introducing any "virus" into RONA's systems or software. If Vendor and/or Vendor's Personnel introduce a virus into RONA systems or software, Vendor will provide assistance to RONA to remove such virus at no additional charge and will reimburse RONA for all damages it incurs in such removal and/or as a consequence of the virus. For the purposes of this Addendum and the Agreement, "virus" includes software routines, codes, instructions, hardware components or combinations thereof, that: (a) permit unauthorized access to RONA systems or software; or (b) disable, delete, modify, damage, or erase software, hardware or data, including components commonly referred to as "viruses," "back doors," "time bombs," "Trojan Horses," "worms" and/or "drop dead devices."

j. Vendor will not insert into any software used by it or supplied pursuant to a statement of works, any code or other device which would have the effect of disabling, damaging, erasing, delaying or otherwise shutting down all or any portion of the services under the Agreement or the hardware, software or data used in providing the services under the Agreement. Vendor will not invoke such code or other device at any time, including upon expiration or termination of this Agreement for any reason.

Notice. The parties agree that any notice by RONA pursuant to this Addendum shall not be required in the form set forth in the Agreement and that email notice to Vendor's Privacy Contact is deemed sufficient.

3. **Certification**. Vendor certifies that it understands and will comply with the restrictions set forth in this Addendum and the Agreement.

4. **Survival**. To the extent that Vendor continues to have access to Confidential and Personal Information and for any reason, Vendor shall continue to be bound by the terms of this Addendum even after termination of the Agreement.