

## **SERVICES AGREEMENT**

This Services Agreement (this “**Agreement**”) is signed as of the signature date(s) below and made effective as of January 1, 2023 (the “**Effective Date**”) by and between Client's Vision Care division of Client Inc., (“**Buyer**”), and Supplier1 (**Supplier**”).

**WHEREAS**, Supplier is in the business of providing media production services and related deliverables and Buyer wishes to engage Supplier for such types of services; and

**NOW, THEREFORE**, in consideration of the premises and of the mutual promises and covenants herein contained, the parties hereto agree as follows:

### **1. SUPPLY OF SERVICES**

- 1.1 Services. During the term of this Agreement, Supplier shall provide Buyer (a) the services, including any deliverables, and (b) the SaaS Services (as defined and set forth in Exhibit H attached hereto), each as more particularly described and set forth in the Statement of Work (the “**SOW**”) attached hereto as Exhibit A (collectively, the “**Services**”).
- 1.2 Updates. Supplier shall, on at least a monthly basis or upon request, provide Buyer with written updates as appropriate to the nature of the Services and the status of remaining Services.
- 1.3 Changes to Services. No changes shall be made to the Services without a written amendment signed by both parties. Buyer is not responsible for any additional fee for any change unless the change order expressly identifies the amount of the additional fee.
- 1.4 Non-Exclusivity. The relationship between Supplier and Buyer is not one of exclusivity.
- 1.5 Supplier Personnel.
  - a. Supplier’s personnel shall complete any required Buyer assigned training on Buyer’s standard operating procedures, policies, systems and requirements in a timely manner. All costs associated with such training shall be included in the fees set forth in the SOW.
  - b. Buyer reserves the right to reject for any lawful reason any of Supplier's personnel assigned by Supplier to provide Services. Supplier shall, as soon as possible thereafter, provide a replacement satisfactory to Buyer. If Supplier’s personnel are identified in the SOW as “**Key Personnel**”, such Key Personnel shall not be reassigned or removed without prior written consent of Buyer. Whenever, for any reason, any such Key Personnel cannot or is unwilling to provide Services, Supplier shall, with prior written approval of Buyer, replace such Key Personnel with personnel of substantially equal abilities and qualifications. In no event shall performance of the Services be delayed or shall Buyer be charged for any time required for any replacement Supplier personnel, including Key Personnel, to be trained to provide or become familiarized with the Services, whether or not the replacement is requested by Buyer.
- 1.6 Buyer Premises. While on Buyer’s or its affiliates’ premises, Supplier shall comply with all rules and regulations of Buyer and those applicable to the premises. Supplier shall be responsible for its personnel and agents while on such premises whether or not any actions fall outside the scope of employment or engagement.
- 1.7 Materials and Equipment. Upon Buyer’s request, Supplier shall promptly return to Buyer all material and equipment provided by Buyer to Supplier.



## **2. TERM AND TERMINATION**

- 2.1 Term of Agreement. This Agreement will be effective on the Effective Date and will expire on December 31, 2023, unless sooner terminated as provided herein or extended in writing by the parties.
- 2.2 Termination of Agreement. Buyer may terminate this Agreement at any time and for any reason upon written notice to Supplier.
- 2.3 Termination for Cause. Buyer or Supplier may terminate this Agreement if the other party is in default of any of its material obligations hereunder and such default is not cured within 10 days after written notice thereof to such party by the party seeking termination; provided, however, there is no cure period for a default that: (a) is the result of negligence or willful misconduct; (b) in the reasonable opinion of the party seeking termination, cannot reasonably be cured; or (c) results in irreparable or continuing harm to the party seeking termination.
- 2.4 Effect of Termination. In the event of any termination, Supplier shall cease all Services under this Agreement after receipt of written notice from Buyer unless such notice expressly provides otherwise and shall cooperate to provide a smooth transition, including, without limitation, such reasonable transition assistance as required by Buyer in order to migrate to another vendor or software solution. If the Agreement is terminated by Buyer for any reason other than pursuant to Section 2.2, Supplier shall provide such transition assistance at no additional charge, and if the Agreement is terminated by Buyer pursuant to Section 2.2, Supplier shall provide such transition assistance as Services. Within 5 days from the effective date of termination, Supplier shall provide to Buyer all material and equipment provided by Buyer to Supplier and all Buyer Materials (as defined in Section 5.6 below), including any work-in-progress and all full and partial copies thereof. Except where Buyer terminates for cause: (a) Supplier shall, within 30 days from the effective date of termination, submit an invoice for all Services performed and all non-cancellable expenses incurred in accordance with this Agreement prior to the effective date of termination and (b) Buyer shall pay such invoice in accordance with the payment terms in Section 3.2.

## **3. PRICE AND PAYMENT**

- 3.1 Pricing and Expenses. Pricing (including any rebates and discounts) is set forth in the SOW. Buyer shall not be required to reimburse Supplier for any expenses or pass through costs unless approved in writing, in advance by Buyer. Buyer shall not be responsible at any time for any mark-up on any expenses of Supplier. All reimbursable travel and reasonable out-of-pocket expenses must be included in the applicable Work Order, must be booked through Buyer's travel group and incurred in accordance with Buyer's travel and expense policies, which Buyer shall provide following a written request by Supplier.
- 3.2 Invoicing and Payment. Unless Buyer provides alternate written instructions, Supplier shall submit all invoices by completing the on-line form on the web site located at <http://www.ap.jnj.com/>. Supplier shall include the following on all invoices: (a) a reference to this Agreement (b) a description of the Services, (c) the price, (d) the purchase order number, (e) expenses and pass-through costs, and (f) sales or use taxes, if applicable. Supplier shall not send any invoices, and no claim from Supplier for payment will be allowed, prior to Buyer issuing a purchase order to Supplier. Payment terms will be net 60 days after Buyer's receipt of an undisputed invoice from Supplier, provided however, the actual payment to Supplier from Buyer or its designee will not be made until the next scheduled payment run as set forth at <http://www.ap.jnj.com/>. Buyer shall not be obligated to pay any amounts not properly invoiced within 90 days after Services are provided, including any pass-through expenses or taxes that otherwise would have been reimbursable in accordance with this Agreement.

## **4. REPRESENTATIONS AND WARRANTIES**

Supplier represents and warrants that:



- 4.1 Services will be performed in accordance with and conform to this Agreement and any applicable industry standards and practices;
- 4.2 The Services shall be physically provided to Buyer inside of Canada;
- 4.3 Supplier is not a "non-resident" for the purposes of the Income Tax Act (Canada);
- 4.4 Services will be provided by qualified personnel, suitably skilled, and trained in the performance of the Services and performed in a diligent and professional manner;
- 4.5 Supplier shall comply with, and the Services will be in compliance with, applicable Buyer policies, all applicable law, statutes, ordinances and regulations, and Supplier shall have any required permits, licenses and certifications applicable to the Services;
- 4.6 Supplier (a) has the full right, power and authority to enter into this Agreement without the consent of a third party, and (b) is under no obligation to any third party, nor will it enter into any obligation with a third party, that could interfere with the Services;
- 4.7 Supplier and the Services, including Supplier Materials (as defined in Section 5.7 below) and Buyer Materials, and the use thereof by Buyer, will not infringe or misappropriate any third party Intellectual Property Rights (as defined in Section 5 (Confidential Information; Intellectual Property Rights)) or violate any duty of confidentiality Supplier has to a third party;
- 4.8 Supplier shall comply with all applicable accessibility laws and regulations, including, but not limited to Accessibility for Ontarians with Disabilities Act, and shall complete and provide evidence of appropriate training on same from time to time as determined by Buyer;
- 4.9 Supplier shall not perform any actions that are prohibited by local and other anti-corruption laws (collectively "**Anti-Corruption Laws**") that may be applicable to one or both parties to this Agreement. Without limiting the foregoing, Supplier shall not make any payments, or offer or transfer anything of value, to any government official or government employee, to any political party official or candidate for political office or to any other third party related to the transaction in a manner that would violate Anti-Corruption Laws;
- 4.10 In performing under this Agreement, Supplier agrees to adhere to the Client's Responsibility Standards for Suppliers (posted on client.com: Responsibility Standards for Suppliers; <https://www.jnj.com/partners/responsibility-standards-for-suppliers>).
- 4.11 Supplier shall comply with Exhibit B (Protection of Personal Information);
- 4.12 Supplier shall comply with Exhibit C (Data Safeguards);
- 4.13 Supplier shall comply with Exhibit D (Health Care Compliance Provisions);
- 4.14 Supplier shall comply with Exhibit E (Pharmacovigilance); and
- 4.15 Supplier shall comply with Exhibit F (Vulnerability Assessment Requirements).

## 5. **CONFIDENTIAL INFORMATION; INTELLECTUAL PROPERTY RIGHTS**

- 5.1 Definition of Confidential Information. As used herein, "**Confidential Information**" includes all information given to one party (the "**Receiving Party**") or its affiliates by the other party or its affiliates (the "**Disclosing Party**") or otherwise acquired by the Receiving Party or its affiliates, in connection with this Agreement, and all information derived or generated therefrom, including (a) information regarding any of the products of the Disclosing Party or any of its affiliates, (b) information regarding costs, productivity or technological advances and (c) this Agreement, any Services and any other information in connection therewith. Buyer Data (as defined in Exhibit H attached hereto) shall be deemed Buyer Confidential Information.



- 5.2 Exceptions. The Receiving Party has no obligation to protect the following categories of Disclosing Party information: (a) information that is or was independently developed by the Receiving Party without use of or reference to any of the Disclosing Party's Confidential Information, as demonstrated by files in existence at the time of disclosure; (b) information that is or was lawfully received from a third party without any restriction on use; or (c) information that becomes or was a part of the public domain through no breach of this Section (Confidential Information; Intellectual Property Rights) by the Receiving Party.
- 5.3 Restrictions on Use and Disclosure. The Receiving Party shall not, except as otherwise provided below (a) use or reproduce the Disclosing Party's Confidential Information for any purpose other than as required to perform the obligations or exercise the rights granted in connection with this Agreement or (b) disclose the Disclosing Party's Confidential Information to any third party, without the prior written approval of the Disclosing Party, except to personnel, consultants, agents and representatives of the Receiving Party or its affiliates who have a need to know such information in connection with the Services and who are bound by obligations of confidentiality at least as restrictive as those set out herein; provided the Receiving Party shall be responsible for any actions of such parties that would be in breach of this Agreement if done by the Receiving Party. Notwithstanding the foregoing, the Receiving Party may disclose the Disclosing Party's Confidential Information to the extent such information is required to be disclosed by law, including a subpoena, or to respond to a regulatory request; provided that the Receiving Party promptly notifies the Disclosing Party in writing prior to any disclosure to allow the Disclosing Party to seek a protective order or similar relief in the Disclosing Party's sole discretion. The Receiving Party shall cooperate fully with the Disclosing Party to appropriately protect against or limit the scope of such requested disclosure.
- 5.4 Protection of Confidential Information. The Receiving Party shall (a) use at least the same degree of care that the Receiving Party uses to protect its own proprietary information of a similar nature and value, but no less than reasonable care to protect and maintain the Disclosing Party's Confidential Information and (b) as requested by the Disclosing Party, return or destroy all of the Disclosing Party's Confidential Information in the Receiving Party's possession or control. Nothing in this Section (Protection of Confidential Information) shall require the destruction or alteration of computer back-up tapes or similar storage made in the ordinary course of the Receiving Party's business that contain the Disclosing Party's Confidential Information, provided that Receiving Party shall continue to comply with its obligations herein with respect to such Confidential Information.
- 5.5 Ownership of Confidential Information. The Receiving Party acknowledges that, except as otherwise provided below, (a) the Disclosing Party is the exclusive owner of and has all rights to its Confidential Information, including all intellectual property rights therein, such as patents, copyrights, trade secrets, trademarks, moral rights and similar rights of any type under the laws of any governmental authority (collectively, "**Intellectual Property Rights**") and (b) no right, title, interest or license to the Receiving Party is either granted or implied under any Intellectual Property Rights by the disclosure of Confidential Information hereunder.
- 5.6 Buyer Materials. Buyer will be the exclusive owner of all deliverables provided under this Agreement and all Intellectual Property Rights therein (collectively, the "**Buyer Materials**"). All Buyer Materials shall constitute the Confidential Information of Buyer. Upon Buyer's request at any time, Supplier shall provide to Buyer all material, data and work-in-progress in connection with the Buyer Materials. Except as set forth in the SOW, Supplier shall not use any Buyer Materials after the effective termination date of this Agreement.
- 5.7 Supplier Materials. Supplier shall retain all Intellectual Property Rights in and to all of Supplier's pre-existing materials, products, software or other property and any of the foregoing that are developed independently of the Services without use of Buyer's or its affiliates' Confidential Information or Intellectual Property Rights (collectively, the "**Supplier Materials**"). Supplier has listed in the SOW all Supplier Materials that Supplier will incorporate into the Buyer Materials or that may be necessary for the full utilization of the Services or Buyer Materials, describing each item in reasonable detail. Supplier hereby grants Buyer and its affiliates a royalty-free, irrevocable, worldwide, paid-up, non-exclusive license to use, copy, disclose, modify, enhance, create derivative works (and own the derivative portion but not the unmodified version) of, license, sublicense

and distribute Supplier Materials incorporated into the Buyer Materials or necessary for the full utilization of the Services and to authorize third parties to do so on their behalf.

- 5.8 Assignment of Rights. To the extent Buyer does not otherwise acquire or retain ownership of Intellectual Property Rights, Supplier hereby irrevocably assigns to Buyer for no additional consideration, and shall cause its personnel to irrevocably assign to Buyer, all right, title and interest in and to the Buyer Materials and all Intellectual Property Rights therein and thereto, including the right to sue, recover damages and obtain other relief from other persons for any past, present and future infringement, dilution, misappropriation, or other violation of or conflict with any of those Intellectual Property Rights. To the extent, if any, that the foregoing assignment and agreement to assign is invalid or if any rights to Buyer Materials cannot be assigned, including moral rights, Supplier irrevocably waives and agrees not to exercise such rights, and Supplier hereby grants to Buyer and its designees the exclusive, transferable, perpetual, irrevocable, worldwide and royalty free right to make, use, market, modify, distribute, transmit, copy, sell, practice, and offer for sale and import the Buyer Materials and any process, technology, software, article, equipment, system, unit, product or component part in connection with the Buyer Materials. At Buyer's request, Supplier will execute any instrument, or obtain the execution of any instrument, including from any employee or contractor, that may be appropriate, and shall provide Buyer all source code and other documents detailing the design and operation of the Buyer Materials, in whatever format Buyer may reasonably require, to assign the rights to Buyer in accordance with this Section (Assignment of Rights) or perfect such rights in Buyer's name. If Supplier fails to execute any assignment in accordance with this Section (Assignment of Rights) within 15 days after a request by Buyer, Supplier hereby grants Buyer power of attorney for the sole purpose of executing any such assignment on behalf of Supplier to Buyer. Supplier shall assist Buyer, at Buyer's expense and as Buyer may request, in any proceeding or litigation involving the Buyer Materials.
- 5.9 Equitable Remedies. Each of the parties hereto acknowledges that a breach of any of the provisions of this Section (Confidential Information; Intellectual Property Rights) could cause irreparable harm to the other party that may be not compensable by a monetary award. Accordingly, the parties acknowledge that, in the event of a breach or threatened breach, the non-breaching party shall be entitled, in addition to any other right or remedy, to seek equitable relief, including injunctions and specific performance without a requirement to post a bond or other security.
- 5.10 No Publicity. Neither party may originate any publicity, news release, technical article, advertising or other announcement, written or oral, whether made to the public press or others (each, an “**Announcement**”), relating to performance under this Agreement or the existence of this Agreement between the parties, except where required by law or as agreed upon in writing by the parties. If required by law to make any Announcement, the party required to do so shall always (a) consult with the other party in connection with said Announcement a reasonable time prior to its release to allow the other party to comment thereon and to prevent its release if so permitted by law; and (b) promptly provide the other party with a copy of the released Announcement and all materials relating thereto. Without limiting the foregoing, neither party may use the names, logos or trademarks of the other party or its affiliates for any advertising or promotional purposes.

## 6. INDEMNIFICATION

- 6.1 Mutual Indemnity Obligations. Each party (each, in such capacity, the “**Indemnifying Party**”) shall indemnify and hold harmless the other party, its affiliates and its agents, and successors and permitted assigns thereof (each, in such capacity, the “**Indemnified Parties**”), against any and all third party claims and resulting liabilities, damages, losses and expenses, including reasonable attorneys' fees, arising out of the following by the Indemnifying Party or its personnel, agents or representatives (a) negligence or willful misconduct in connection with this Agreement or (b) a breach of this Agreement.
- 6.2 Intellectual Property Indemnity. Supplier, at its sole expense, shall defend, indemnify and hold harmless the Buyer Indemnified Parties against any and all claims, demands, suits or proceedings threatened or asserted against the Buyer Indemnified Parties relating to the Services or deliverables for infringement, misuse,



misappropriation, or violation of any copyright, trademark, service mark, trade secret, patent or other intellectual property or proprietary right of a third party (each an "**Infringement Claim**").

6.2.1. If the Services or deliverables become subject to any Infringement Claim, then Supplier shall, at Supplier's expense, obtain for Buyer the right to continue its use of the Services or deliverables as provided herein free of any such claim or action. If Supplier, despite using its best efforts, is unable to obtain such right for Buyer, then Supplier shall, at Supplier's expense, replace or modify the Services or deliverables so that it becomes non-infringing; provided, however, that the replaced or modified Services or deliverables shall be similar in all material respects and functionally equivalent to the Services and deliverables being replaced.

6.2.2. Any replaced or modified Services or deliverables provided under this Section 6.2.1 are subject to all of the terms and conditions of this Agreement, including without limitation, the indemnification provisions of this Section 6 (Indemnification).

6.2.3. If Supplier, despite using its reasonable efforts, is unable to take the measures set forth above, and Supplier is subsequently permanently enjoined from providing or licensing the Services or deliverables to Buyer, then, in addition to Supplier's other obligations set forth in this Section 6 (Indemnification), Supplier shall accept return of the Services and deliverables from Buyer and pay an amount equal to the fees paid with respect to the Services and deliverables.

6.3 Indemnity Procedures. The Indemnified Parties will give the Indemnifying Party prompt written notice of any matter upon which the Indemnified Parties intend to base a claim. With respect to the settlement of any claim relating solely to the payment of money damages, which could not result in the Indemnified Parties becoming subject to injunctive or other equitable relief or otherwise adversely affect the business of the Indemnified Parties in any manner, and as to which the Indemnifying Party has acknowledged in writing its obligation to indemnify the Indemnified Parties hereunder, the Indemnifying Party shall have the sole right to settle or otherwise dispose of such claim, on such terms as the Indemnifying Party shall deem appropriate, provided that Indemnifying Party shall provide reasonable evidence of its ability to pay any damages claimed and, with respect to any such settlement, shall have obtained the written release of the Indemnified Parties from the claim. The Indemnified Parties may participate in such negotiations to protect their interests and the Indemnifying Party will provide reasonable assistance to the Indemnified Parties and their counsel at no charge. With respect to the settlement of any claim not relating solely to the payment of money damages, the Indemnifying Party will have the right to consent to the entry of judgment with respect to, or otherwise settle, a claim only with the prior written consent of the Indemnified Parties, which consent will not be unreasonably withheld, provided, however, that the Indemnified Parties may withhold consent if any such judgment or settlement imposes an unreimbursed monetary or continuing non-monetary obligation on such Indemnified Parties or does not include an unconditional release of the Indemnified Parties from all liability with respect to the claim.

## **7. LIMITATION OF LIABILITY**

IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY PUNITIVE, EXEMPLARY, MULTIPLIED, INDIRECT OR CONSEQUENTIAL DAMAGES, LOST PROFITS OR REVENUES OR ANY CLAIM FOR ANY PREJUDGMENT INTEREST; PROVIDED THAT THE FOREGOING LIMITATIONS DO NOT APPLY TO (a) INDEMNIFICATION OBLIGATIONS PURSUANT TO SECTION 6 (INDEMNIFICATION) OR (b) ANY BREACH OF EXHIBIT I (PROTECTION OF PERSONAL INFORMATION).

## **8. INSURANCE**

8.1 Coverage. During the Term of this Agreement and thereafter, Consultant agrees to maintain at its own expense, professional and general liability insurance coverage of the nature and amounts commercially reasonable to sufficiently cover claims that could reasonably arise given the nature of this Agreement.





8.2 Cancellation Notice. All such policies of insurance shall include an endorsement providing that no cancellation of any such policy will be effective unless Buyer received at least 30 days' prior written notice of such cancellation.

8.3 Certificates of Insurance. Consultant shall cause a certificate(s) of insurance executed by the insurer named in the applicable policies described above (or by an authorized insurance broker) to be delivered to Buyer concurrently with Consultant's execution of this Agreement and from time to time following the receipt of a written request therefor from Buyer.

## **9. GOVERNING LAW; DISPUTE RESOLUTION**

9.1 Governing Law. This Agreement and SOW are governed by and will be construed in accordance with the laws of the Province of Ontario and the federal laws of Canada, excluding any conflicts of law provisions. Subject to the Section below (Mediation), the parties hereby irrevocably attorn to the jurisdiction of the courts of the Province of Ontario.

9.2 Mediation. Any controversy or claim arising out of or relating to this Agreement, including any such controversy or claim involving the parent company, subsidiaries, or affiliates under common control of any party (a "**Dispute**"), shall first be submitted to mediation according to International Centre for Dispute Resolution – Canada's ("**ICDR Canada**") Canadian Mediation Rules. Such mediation shall be attended on behalf of each party for at least one session by a senior business person with authority to resolve the Dispute. Any period of limitations that would otherwise expire between the initiation of mediation and its conclusion shall be extended until 20 days' after the conclusion of the mediation. All aspects of the mediation shall be kept confidential.

9.3 Arbitration. Any controversy or claim arising out of or relating to the Agreement, or the breach of the Agreement, that is not resolved through mediation shall be settled by arbitration by a single arbitrator administered by ICDR Canada in accordance with the Canadian Arbitration Rules. The seat of the arbitration shall be Toronto, Ontario and the language of the arbitration shall be English. The arbitrator shall apply the substantive law of Ontario. The proceedings of the arbitration shall be confidential and there shall be no appeal from the award rendered by the arbitrator, judgment on which may be entered in any court having jurisdiction.

9.4 Injunctive Relief. Nothing in this Section (Governing Law; Dispute Resolution) restricts or prohibits either party from seeking urgent relief from a court of competent jurisdiction to preserve a legal right or remedy, or to protect a proprietary trade secret right, or to otherwise seek emergency legal or equitable remedies necessary to preserve or restore the status quo pending the outcome of arbitration or mediation, and no such court action shall be deemed a waiver of the requirement to mediate or arbitrate Disputes pursuant to this Section (Governing Law; Dispute Resolution).

## **10. RELATIONSHIP OF THE PARTIES**

The relationship of the parties established by this Agreement is that of independent contractors and nothing contained herein will be construed to (a) give either party any right or authority to create or assume any obligation of any kind on behalf of the other party or (b) constitute the parties as partners, joint ventures, co-owners or otherwise as participants in a joint or common undertaking. This Agreement constitutes a contract for the provision of Services and not a contract of employment of Supplier or any Supplier personnel.

## **11. FORCE MAJEURE**

If any party is affected by any event beyond its reasonable control, including (a) fire, explosion, flood or other act of God, (b) acts, regulations or laws of any government, (c) war, terrorist acts or civil commotion or (d) failure of public utilities or common carriers (a "**Force Majeure Event**"), such party shall not be liable in connection with this Agreement to the extent affected by such Force Majeure Event; provided such party gives prompt written notice to the other party (the "**Non-Force Majeure Party**") of the Force Majeure Event and such affected party exercises all



reasonable efforts to eliminate the effects of the Force Majeure Event on this Agreement as soon as possible. If any Force Majeure Event continues for a period longer than 30 days, the Non-Force Majeure Party may terminate the affected Work Order upon written notice to the other party.

## **12. SUBCONTRACTORS**

Supplier shall not subcontract any of its obligations hereunder, including to any affiliate, without the prior written consent of Buyer. Supplier shall be responsible for (a) ensuring that any permitted subcontractors comply with this Agreement, (b) all actions of such subcontractors in connection with this Agreement, including any actions that would be in breach of this Agreement if performed by Supplier and (c) all payments due to permitted subcontractors, all materials, equipment and labor used by permitted subcontractors in providing the Services and keeping Buyer's premises and equipment free of all liens. Buyer shall have the right, upon notice to Supplier, to make any payments that Buyer reasonably believes to be due to permitted subcontractors directly to such permitted subcontractors, and to deduct the amount of any such payments made from any amounts due to Supplier.

## **13. ASSIGNMENT**

Supplier shall not assign this Agreement without the prior written consent of Buyer and any attempt to do so will be void. This Agreement is intended solely for the benefit of the parties hereto, and it is not the intention of the parties to confer third-party beneficiary rights upon any other person or entity. Subject to the foregoing, this Agreement will bind and inure to the benefit of the parties hereto and their respective successors and permitted assigns.

## **14. AUDIT**

14.1 Buyer or Buyer's authorized representative and any governmental agency which regulates Buyer may, at all reasonable times during the term of the Agreement and for 3 years thereafter and upon reasonable notice, inspect and audit the books and records of Supplier with respect to the Services for the sole purpose of evaluating Supplier's compliance with this Agreement and any law, regulation or policy applicable to Buyer. Supplier shall retain all applicable books and records for 3 years subsequent to the expiration or termination of this Agreement or such longer period as required by applicable local or international regulatory requirements. Supplier shall respond within 1 business day of receipt of Buyer's request with information and documentation required in relation to any regulatory authority inspection. Supplier shall also provide Buyer with reasonable cooperation and access to those portions of the facilities in which Services are performed for Buyer and to appropriate Supplier personnel, Supplier's information systems, and privacy and security procedures. Supplier shall also, within 10 days after Buyer's written request, provide annual certifications of Supplier's compliance with the policies and obligations set forth in the Agreement.

14.2 Service Organization Controls Report(s). At Supplier's cost, Supplier shall provide independent assurance over business and information technology controls performed under the Agreement by providing a Service Organization Controls Report based on the American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements No. 18 (SSAE 18) ("SOC Report(s)"). Such SOC Report(s) will cover all controls that Supplier and subservice organizations perform under the Agreement and be in the form of a SOC 1 Type II and SOC 2 Type II report. The reporting period for the SOC Report(s) will be each calendar year. Supplier shall provide Buyer and Buyer's external auditor with copies of relevant reports upon issuance; provided, however, Supplier shall use reasonable efforts to deliver such SOC Report(s) no later than November 15. To bridge any gap between the service audit end date and December 31 of each year, Supplier shall provide Buyer an additional affirmation of ongoing control operating effectiveness. If a SOC Report from the retained third-party auditors yields deviations, Supplier shall communicate an action plan within 30 days of the SOC Report issuance and provide Buyer periodic updates until the deviations have been remediated, retested and deemed resolved by the third-party auditors. Supplier shall comply with future guidance relating to SOC Reports as issued by the AICPA Auditing Standards Board (ASB).

## **15. RECORDS AND INFORMATION MANAGEMENT ("RIM") REQUIREMENTS**

Supplier shall comply with Exhibit G (Records and Information Management ("RIM") Requirements).





## **16. TAXES**

16.1 All fees charged by Supplier shall be exclusive of value added, sales, use, goods and services, transfer, services, consumption or transaction taxes (“**Indirect Taxes**”), as well as gross receipts, excise and other taxes. Buyer shall make all payments of fees to Supplier under this Agreement without deduction or withholding for any tax, unless such deduction or withholding is required by law. Each party shall be responsible for: taxes based on its own income (“**Income Taxes**”); gross receipts, capital stock, and net worth taxes; franchise and privilege taxes on its business; employment taxes of its employees; and taxes on any property it owns or leases. Supplier shall not pass on to Buyer and Buyer shall not be responsible for any taxes that Supplier incurs in subcontracting the performance of the Services except to the extent such taxes are included in the pricing set forth in this Agreement. Buyer and Supplier will reasonably cooperate with each other to more accurately determine a party’s tax liability and to minimize such liability, to the extent legally permissible.

16.2 In the event applicable law requires Buyer to withhold any Income Taxes from any payments made to Supplier, then Buyer shall withhold such Income Taxes, pay the full amount withheld to the relevant taxing authority, and provide Supplier with proof of such payment. Any such Income Tax required to be withheld shall be an expense of and borne by Supplier and any amounts paid, deducted or withheld by Buyer shall be treated for all purposes of this Agreement as paid to Supplier.

16.3 Supplier may charge Buyer for Indirect Taxes, as long as the amount of Indirect Taxes are specified in a valid invoice compliant with applicable law. Buyer shall either pay such invoiced amount or supply valid exemption documentation. If Supplier does not provide Buyer with a valid invoice (including separate identification of Indirect Taxes where required by applicable law), Supplier shall assume responsibility for such non-compliance, including payment of any tax-related interest and penalties. Supplier shall segregate on the invoice fees for taxable Services from fees for nontaxable Services.

16.4 Canadian Tax Reporting. A T4A form from the Canada Revenue Agency will be issued to the Supplier, whether Supplier is a sole proprietorship, a partnership, or a limited liability corporation, and Supplier shall have established a name that it uses to carry on business. Buyer shall report income on the T4A form for amounts paid not including VAT, GST/HST, sales, use or other similar tax charged by the Supplier, and by Canada Revenue Agency guidelines. The T4A form is not subject to tax deductions or withholdings.

## **17. HEADINGS**

The headings used herein have been inserted for convenience only and do not affect the interpretation of this Agreement.

## **18. WAIVER**

No party shall be deemed to have waived any provision of this Agreement except pursuant to a written waiver executed by the waiving party. The failure of any party to enforce at any time for any period any provision hereof will not be construed to be a waiver of such provision or of the right of such party thereafter to enforce each such provision, nor shall any single or partial exercise of any right or remedy hereunder preclude any other or further exercise thereof or the exercise of any other right or remedy.

## **19. SEVERABILITY**

Any provision of this Agreement that is invalid or unenforceable in any jurisdiction will, to the extent the economic benefits conferred thereby to both parties remain substantially unimpaired, be ineffective to the extent of such invalidity or unenforceability without rendering invalid or unenforceable the remaining provisions or affecting the validity or enforceability of any of such provisions in any other jurisdiction.



## **20. NOTICES**

To be effective, all notices in connection with this Agreement must be in writing and sent to the parties at the addresses below, or to such other place as a party may designate by written notice to the other parties, and shall be deemed to have been given upon: (i) receipt if delivered by personal delivery; (ii) the third business day after being sent by certified or registered mail, return receipt requested, postage prepaid; (iii) the second business day after being sent by overnight courier, billed to sender; or (iv) the second business day after sending by email provided that there is no error message sent to, or received by, the sender. Each party may modify its recipient of notices by providing notice pursuant to this Section.

*Supplier:*

*Buyer:*

## **21. PHARMACOVIGILANCE**

Supplier shall perform pharmacovigilance reporting in accordance with Exhibit E (Pharmacovigilance Obligations) attached hereto.

## **22. ENTIRE AGREEMENT; CONFLICTS**

22.1 Entire Agreement. This Agreement (a) supersedes all previous understandings, agreements and representations between the parties, written or oral and (b) constitutes the entire agreement and understanding between the parties with respect to the subject matter hereof, and incorporates all representations, warranties, covenants, commitments and understandings on which they have relied in entering into this Agreement. No modification, change or amendment to this Agreement shall be effective unless in writing and signed by each of the parties.

22.2 Conflicts. No terms and conditions of any purchase order or provision included in any invoice, estimate, confirmation, acceptance or any other similar document in connection with this Agreement will be effective unless expressly stated otherwise in a writing signed by each of the parties. Any additional provisions in accordance with the foregoing shall expressly be subject to this Agreement. To the extent of any conflict or inconsistency between this Agreement and such provisions, this Agreement shall govern, unless such writing includes the section number of this Agreement that the parties agree no longer governs or is modified for the matter covered thereby.

## **23. SURVIVAL**

The following sections survive any termination or expiration of this Agreement and any termination or completion of any or all SOWs: 2.4, 4 to 10 inclusive, 15, 17 and any other provisions that by their nature and context are intended to survive.

## **24. COUNTERPARTS; ELECTRONIC SIGNATURES**

This Agreement may be executed in two or more counterparts, each of which shall be deemed an original, and all such counterparts together shall constitute one and the same instrument. Electronically executed or electronically transmitted (including via fax or pdf) signatures shall have the full force and effect of original signatures.

**25. REMEDIES**

Subject to Sections 9 (Governing Law; Dispute Resolution) and 7 (Limitation of Liability), any remedies provided herein are cumulative and not exclusive of any remedies provided by law or equity.

**IN WITNESS WHEREOF**, the parties have caused this Agreement to be executed by their duly authorized representatives.



## **EXHIBIT A – STATEMENT OF WORK**

### **Project: "2023 Orion/Pitcher/Video Services/Creation Services"**

#### **Objective:**

Supplier will develop, edit and manage the art, layouts, & media materials for each brand (“**Sales Aid Materials**”) for the various versions of the existing Canadian sales force HTML5 based sales app; assist with the upload of Sales Aid Materials into the sales app; and maintain the JJV Canada Dashboard (Dale).

Supplier will provide the following Services and deliverables:

#### **1. Services and Deliverables:**

##### **1.1 Services**

- i. Develop and deliver all new Canadian sales force html5 based Sales Aid Materials monthly for all of 2023 and upload into Orion/Pitcher sales app.
- ii. Develop and deliver future Orion/Pitcher Sales Aid Materials throughout 2023.
- iii. Edit and deliver Orion/Pitcher revised Sales Aid Materials as required by Buyer.
- iv. Create flat file copy clearance documents.
- v. Assist with uploading the Sales Aid Materials to the Orion/Pitcher UA sandbox instance and production instance.
- vi. Deliver a major Sales Aid Materials overhaul for each brand.
- vii. Deliver quarterly Sales Aid Materials maintenance for each brand.
- viii. Edit and maintain JJV Canada Dashboard (Dale).

##### **1.2 Deliverables**

- i. Deliver and upload all new html5 monthly for all of 2023 into Orion/Pitcher
- ii. Deliver future revision and Orion/Pitcher builds throughout 2023
- iii. Deliver Orion/Pitcher sales aid edits as required

#### **2. Supplier's Personnel:**

- a. Authorized Personnel. The following personnel of Supplier are authorized to provide Services on behalf of Supplier: None
- b. Personnel Qualifications. Supplier personnel providing the Services shall at least meet the following qualifications: None

#### **3. The project managers are:**

Supplier Contact Information:

Buyer Contact Information:



4. **Acceptance:** Buyer shall have the right to review and, if applicable, test each deliverable for the functional requirements or acceptance criteria specified for such deliverable. Supplier shall promptly cure, in a manner agreed upon by Buyer, any deficiencies to which Supplier has been made aware, and after completing any such cure, Supplier shall resubmit the deliverable for review and, if applicable, testing. Any applicable warranty period shall only commence after acceptance by Buyer.

5. **Supplier Materials:**

Pursuant to Section 5.7 of the Agreement, the following Supplier Materials are incorporated into Buyer Materials: None

6. **Pricing:**

**Fixed Fee:** The total fee Supplier shall charge for Services provided under this SOW including all expenses \$110,000.00 CAD, which shall be invoiced by Supplier upon completion, delivery, and acceptance by Buyer of Services as follows:

Milestone	Fee (CAD)
Upon Execution of Agreement	\$22,000.00
Upon Completion, Delivery and Acceptance by Buyer of Deliverables	\$88,000.00
<b>Total</b>	<b>\$110,000.00</b>

In no event shall the total fees for Services provided exceed **\$110,000.00 CAD**.

7. **Travel & Other Expenses:**

For any allowable travel expenses that are billable to Buyer, Supplier shall comply with Buyer's travel policy and utilize Buyer Travel Services for all travel arrangements. Contact information for Buyer's Travel Services should be obtained from, and any other questions about Buyer's travel policy should be directed to, Supplier's point of contact for Buyer for the work hereunder.

Any reasonable and customary travel and out-of-pocket expenses will be charged at cost (after Supplier deducts all discounts and rebates it receives); provided, however, Supplier shall (a) receive Buyer's consent prior to incurring any such expenses, (b) incur all such expenses in accordance with Buyer's travel and expense policy, and (c) in no event exceed **\$0.00** for travel and out-of-pocket expenses. Receipts for travel and out-of-pocket expenses in excess of \$25 should be retained and must be produced if requested by Buyer. Supplier shall not bill for travel time without prior approval from Buyer.



## **EXHIBIT B - PROTECTION OF PERSONAL INFORMATION**

### **1. Definitions**

- 1.1. “**2021 SCCs**” means the attached 2021 EU Standard Contractual Clauses ((EU) 2021/914) together with the attached Annexes I and II.
- 1.2. “**Adequacy Decision**” means a decision adopted by a competent authority with jurisdiction over Buyer declaring that a jurisdiction meets an adequate level of protection of Personal Information.
- 1.3. “**Anonymized Data**” means information that does not relate to an identified or identifiable individual or Personal Information (as defined below) rendered anonymous, as defined by applicable law, in such a manner that the individual is not or is no longer identifiable.
- 1.4. “**Data Protection Laws**” means any laws including national implementing legislation, ordinances, rules, regulations and lawful orders of any public authority to which a party is subject, relating to data protection, the Processing of Personal Data, privacy and/or electronic communications.
- 1.5. “**FADP**” means the Swiss Federal Act on Data Protection.
- 1.6. “**GDPR**” means the EU General Data Protection Regulation ((EU) 2016/679).
- 1.7. “**Model Contracts**” means any or all model contract language dictated by a particular jurisdiction and determined to provide a sufficient legal basis for transfers by a competent authority with jurisdiction over such transfers, including the 2021 SCCs, UK 2021 SCCs Addendum, and Argentine Model Clauses.
- 1.8. “**Personal Information**” (or “**Personal Data**”) means data that identifies, can be used to identify, relates to, or is capable of being associated with, or could reasonably be linked, directly or indirectly, with an individual or household, as defined by applicable law, and includes Pseudonymized Data.
- 1.9. “**Privacy Breach**” means any unauthorized access, acquisition, use, alteration, disclosure, loss or destruction of, or damage to, Buyer’s Personal Information, or any breach of applicable privacy or data protection laws, or of the requirements of this Agreement with respect to the Processing of Buyer’s Personal Information by or on behalf of Supplier.
- 1.10. “**Process,**” “**Processed,**” and “**Processing**” means any operation or set of operations performed on Personal Information, whether or not by automatic means, including the collection, creation, possession, use, disclosure, transfer, storage, deletion, combination, access, or other use of Personal Information as contemplated by applicable privacy and data protection laws.
- 1.11. “**Pseudonymized Data**” or “**Pseudonymous Data**” means Personal Information that can no longer be attributed to a specific individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures, to ensure the Personal Information is not attributed to an identified or identifiable individual.
- 1.12. “**Sensitive Personal Information**” (or “**Sensitive Personal Data**”) means Personal Information about an individual’s racial or ethnic origin, religious or philosophical beliefs, trade union membership, political opinions, sexual life or orientation, physical or mental health or medical conditions, criminal record or history, or social insurance number or social security number, citizenship or immigration status, genetic or biometric data processed for the purpose of uniquely identifying an individual, Personal Information collected from a known child, precise geolocation data or as otherwise defined by applicable law.
- 1.13. “**UK 2021 SCCs Addendum**” means UK International Data Transfer Addendum to the 2021 SCCs, Version B1.0, including Part 2 ‘Mandatory Clauses,’ which can be found at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/>, incorporated herein by reference.





- 1.14. “**UK Data Protection Laws**” means all laws, including national implementing legislation, ordinances, rules, regulations and lawful orders of any public authority to which a party is subject, relating to data protection, the Processing of Personal Data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

## 2. **Personal Information Privacy & Data Protection**

**2.1 Processing.** Supplier shall Process Personal Information only to perform its obligations under this Agreement, or as otherwise instructed by Buyer in writing from time to time. Supplier’s Processing of Personal Information shall be governed by the terms of the Agreement, including this Exhibit, the Model Contracts incorporated herein, and Annex I.B to the 2021 SCCs, and related Statements of Work and/or Work Orders, which set out the subject matter, duration, nature, and purpose of the Processing, types of Personal Information, categories of data subjects, and obligations and rights of the Buyer. Supplier is prohibited from using, disclosing, sharing or otherwise selling Personal Information, except as expressly permitted in the Agreement and this Exhibit. Supplier shall Process Personal Information in accordance with all applicable Data Protection Laws, and applicable policies and standards, including, to the extent required as part of Supplier’s obligations under this Agreement, with Buyer’s Cookie Policy. For clarity, and without limiting the generality of the foregoing, in no event may Supplier:

- (a) “sell” or “share” Personal Information (as those terms are defined under applicable Data Protection Law);
- (b) disclose Personal Information to any third party for the commercial benefit of Provider or any third party;
- (c) retain, use, disclose, or otherwise Process Personal Information outside of its direct business relationship with Buyer or for a commercial purpose other than the business purposes specified in the Agreement; or (d) combine Personal Information with personal information that Supplier receives from, or on behalf of, other persons, or collects from its own interaction with an individual, except and solely to the extent expressly permitted under the Data Protection Laws. Supplier certifies that it understands and will comply with the foregoing restrictions.

**2.2 Sensitive Personal Information.** To the extent Supplier stores or transmits Sensitive Personal Information in accordance with the provision of the Services, it shall implement appropriate technical safeguards, including but not limited to data encryption, consistent with the sensitivity of the data and Buyer’s Data Safeguards requirements, as described in Exhibit XX. Supplier shall limit the Processing of Sensitive Personal Information to only that which is strictly necessary to provide desired Services to the Buyer, as determined by the Buyer.

**2.3 Supplier-Provided Data.** To the extent Supplier provides information or data to Buyer in accordance with the Services:

**2.3.1 Pseudonymized Data.** If Supplier provides Pseudonymized Data to Buyer, the following will apply:

- 2.3.1.1 Supplier represents and warrants that when Pseudonymized Data are provided to Buyer, Supplier will not provide Buyer with any key or code that enables such Pseudonymized Data to be re-identified.
- 2.3.1.2 Supplier will notify Buyer immediately (and in any event within twenty-four (24) hours) if Supplier discovers that any non-Pseudonymized Personal Information has been provided to Buyer. Supplier will cooperate with Buyer’s requests to mitigate any harm resulting from any such disclosure of Personal Information and shall promptly deliver corrected Pseudonymized Data to Buyer at no cost to Buyer.

**2.3.2 Anonymized Data.** If Supplier will provide Anonymized Data to Buyer, the following will apply:

- 2.3.2.1 Supplier represents and warrants that any Anonymized Data supplied to Buyer has been anonymized to remove direct identifiers, such that when used in conjunction with other data held by or disclosed to Buyer, cannot be reasonably linked to or used to identify an individual.



2.3.2.2 Where Anonymized Data includes health-related data or information, the following provisions shall apply:

2.3.2.2.1 For patients in the United States, Supplier shall de-identify all Personal Information in accordance with 45 C.F.R. §164.514 of the Health Insurance Portability and Accountability Act, as amended.

2.3.2.2.2 For patients outside the United States, unless otherwise agreed to by the parties, all Personal Information shall be anonymized by Supplier in accordance with Opinion 05/2014 on Anonymization Techniques issued by the Article 29 Working Party (available at [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf)).

2.3.3 Supplier shall notify Buyer immediately (and in any event within twenty-four (24) hours) if Supplier discovers that any Anonymized Data provided to Buyer does not satisfy the requirements set forth herein. Supplier shall cooperate with Buyer's requests to mitigate any harm resulting from any such disclosure of Anonymized Data that do not comply with Section 1.1. Supplier will promptly deliver corrected Anonymized Data to Buyer at no cost to Buyer. Buyer shall not be considered a Data Controller under applicable data protection regulations with respect to the Processing of the Personal Information used as a source for such Anonymized Data.

**2.4 Third Parties.** Supplier will not disclose or transfer Personal Information to, or allow access to Personal Information by (each, a "**Disclosure**") any third party without Buyer's express prior written consent; provided, however, that Supplier may disclose Personal Information to its affiliates and approved subcontractors for purposes of providing the Services to Buyer, subject to the following conditions: (a) Supplier will maintain a list of the affiliates and subcontractors (with contact information) and the Processing activities to be performed in connection with such Disclosures and will provide this list to Buyer upon Buyer's request; (b) Supplier will provide Buyer with at least forty-five (45) calendar days' prior notice of the addition of any third party to this list and the opportunity to object to such addition(s); and (c) if Buyer makes such an objection and Supplier is unable to modify the Services to prevent Disclosure of Personal Information to the additional third party, Buyer will have the right to terminate the relevant Processing. Supplier will, prior to any Disclosure, enter into a written agreement with such third party that is at least as restrictive as this Exhibit. Such agreement will be provided to Buyer promptly upon request. Supplier will remain responsible at all times and will be held liable for all actions by such third parties with respect to the Disclosure.

**2.5 Data Accuracy.** Supplier shall, to the extent required as part of Supplier's obligations under this Agreement, ensure that all Personal Information provided by or on behalf of Buyer and Processed by Supplier is accurate and, where required, kept up-to-date, and ensure that any Personal Information that Supplier is notified, or otherwise has knowledge, is inaccurate or incomplete, is securely erased or rectified in accordance with Buyer's instructions, this Agreement, or applicable law.

**2.6 Data Subject Inquiries.** Supplier shall, unless specifically prohibited by applicable law (i) promptly (and in any event within five (5) calendar days of receipt) notify Buyer in writing if Supplier receives any requests, complaints, or inquiries from an individual with respect to Personal Information Processed by Supplier, including opt-out requests, requests for access, correction, deletion or portability, or to stop the disclosure, sharing or sale of Personal Information, where allowed by law, or allegations that the Processing infringes an individual's rights under applicable law; and (ii) not respond to any such requests, complaints or inquiries unless expressly authorized to do so by Buyer. Supplier will cooperate with Buyer with respect to any action taken relating to an individual's request or complaint and will seek to implement appropriate processes (including technical and organizational measures) to assist Buyer in responding to such requests or complaints. Supplier will promptly and securely delete or destroy any Personal Information pertaining to an individual identified by Buyer where such information is within Supplier's possession or control. If applicable, Supplier will direct any authorized third party (including Supplier's subcontractors and affiliates) that Processes Personal Information related to the identified individual to promptly and securely delete or destroy such Personal Information. If notification to such authorized third party is impossible or would involve disproportionate effort, Supplier shall provide Buyer a detailed explanation that includes enough facts to give an individual a meaningful understanding as to why the



notification was not possible or involved disproportionate effort. Buyer will inform Supplier of any such request that it must comply with and will provide information necessary for Supplier to comply with the request. Supplier will confirm to Buyer in writing that it has complied with its obligations under this section.

**2.7 Privacy Breach.** Supplier shall notify Buyer in writing immediately (and in any event within twenty-four (24) hours) whenever Supplier reasonably believes that there has been a Privacy Breach. Such notice will provide detailed information regarding the Privacy Breach, including its nature and scope; actual or potential cause; any reports to law enforcement; and, measures being taken to investigate, correct, mitigate, and prevent future Privacy Breaches. Supplier will provide, at Supplier's sole cost, reasonable assistance and cooperation requested by Buyer to investigate and notify affected individuals, regulatory bodies, or credit reporting agencies with respect to any such Privacy Breach. Supplier will mitigate the effects of the Privacy Breach as Buyer deems appropriate, including the provision of any credit reporting or other remedial service as required by applicable law or otherwise agreed to by the parties. Supplier shall not notify any individual or any third party of any Privacy Breach without Buyer's prior consent except to the extent required by law and, in such case, Supplier shall notify Buyer within forty-eight (48) hours of notice of any such legal requirement. In addition, within thirty (30) calendar days of identifying or being informed of a Privacy Breach, Supplier shall develop and execute a plan that reduces the likelihood of a recurrence of such Privacy Breach, following submission of such plan to Buyer for review and feedback. To the extent the Privacy Breach resulted from a violation of Supplier's duties under any agreement between Supplier and Buyer, Supplier will (i) assist with curing any alleged violation and ensure that no further violations shall occur, and (ii) provide Buyer with a written statement confirming such cure and no further violations. Without limiting any other rights of Buyer under this Agreement, Buyer may at its discretion immediately terminate this Agreement or the relevant Statement of Work or Work Order as a result of a Privacy Breach without Buyer having any financial or other liability of any nature whatsoever to Supplier resulting from such termination.

**2.8 Return or Destruction of Data.** Supplier shall cease Processing and promptly return, archive, or securely destroy any Personal Information in its possession provided by or on behalf of Buyer, in accordance with Buyer's instructions, when no longer necessary to provide the Services to Buyer, upon termination or expiration of this Agreement, or for any reason immediately upon Buyer's request. When disposing of any paper, electronic or other record containing Personal Information (including Personal Information retained by Supplier for disaster recovery and data back-up), Supplier shall do so by taking all reasonable steps to use industry standard methods to destroy the information such as by: (i) shredding; (ii) permanently erasing and deleting; (iii) degaussing; or, (iv) otherwise modifying the Personal Information in such records to make it unreadable, unreconstructable and indecipherable. Upon request, Supplier shall provide written certification confirming the return or destruction of such Personal Information.

**2.9 Legal Process.** If Supplier is required by law or receives any order, demand, warrant or any other document from a court of competent jurisdiction or other governing body requesting or purporting to compel the production of Personal Information, Supplier shall, except to the extent prohibited by law, immediately notify Buyer and shall not produce the Personal Information for at least forty-eight (48) hours following such notice to Buyer so that Buyer may, at its own expense, exercise such rights as it may have under law to prevent or limit such disclosure. In addition to the foregoing, Supplier shall exercise commercially reasonable efforts to prevent and limit any such disclosure to otherwise preserve the confidentiality of the Personal Information and shall cooperate with Buyer with respect to any action taken with respect to such legal process, including to obtain an appropriate protective order or other reliable assurance that confidential treatment will be accorded to the Personal Information.

**2.10 Review of Policies and Procedures.** At any time during the term of this Agreement, upon request and in a reasonable time and manner and subject to Buyer's confidentiality obligations set forth in the Agreement, Supplier shall make its policies, procedures, practices, and books and records relating to the privacy and security of Personal Information and the Processing of Personal Information available to Buyer and/or its affiliates or their authorized representatives for review.

**2.11 Site Audits.** Supplier shall provide Buyer and its affiliates and their authorized representatives upon reasonable request with: (i) access to Supplier's premises and records; (ii) assistance and cooperation of Supplier's relevant staff; and (iii) facilities at Supplier's premises for the purpose of auditing Supplier's



compliance with its obligations in this Exhibit. When responding to a Buyer-mandated audit or request for information, Supplier shall inform Buyer if Supplier believes that any of Buyer's instructions regarding the Personal Information violates applicable law. Supplier shall also assist and support Buyer in the event of an investigation by any regulatory authority, including a data protection regulator, if and to the extent that such investigation relates to Personal Information Processed by Supplier for Buyer. Such assistance shall be at Buyer's expense, except where such investigation was required due to Supplier's acts or omissions, in which case such assistance shall be at Supplier's expense.

**2.12 Cross-Border Transfers.** Supplier shall ensure that Personal Information is not disclosed to, transferred to and/or allowed to be accessed by or otherwise Processed by its employees or personnel in any country except as set forth in this Agreement or in associated Work Orders, Statements of Work or Purchase Orders, unless previously agreed to in writing by Buyer.

2.12.1 The 2021 SCCs which are incorporated into this Exhibit and Agreement as if fully set forth herein, will apply to any transfer of Personal Information that is subject to the GDPR, UK Data Protection Laws or FADP to Supplier located outside the EEA, United Kingdom ("UK") and Switzerland, as discussed further herein and below, except to the extent the transfer is covered by an Adequacy Decision. Where the transfer relates to Personal Information subject to FADP, all references in the 2021 SCCs to the "Union", "EU," "Member State" will be interpreted as references to Switzerland and references to EU law will be interpreted as relevant provisions of the FADP. Where the transfer relates to Personal Information subject to the UK Data Protection Laws, all references in the 2021 SCCs to the "Union", "EU", or "Member State" will be interpreted as references to the UK and references to EU law will be interpreted as relevant provisions to the UK Data Protection Laws.

- 2.12.1.1 For the purpose of Clause 17 of the 2021 SCCs, the parties agree that the 2021 EU SCCs will be governed by the law of Switzerland for transfer of Personal Information subject to FADP, and by the law of the UK for transfer of Personal Information subject to UK Data Protection Laws.
- 2.12.1.2 For the purpose of Clause 18 of the 2021 SCCs, the parties agree that any dispute arising from the 2021 SCCs will be resolved by the courts of Switzerland for transfers of Personal Information subject to FADP, and by the courts of the UK for transfers of Personal Information subject to UK Data Protection Laws.
- 2.12.1.3 For the purpose of Annex I.C of the 2021 SCCs, the parties agree that Switzerland's Federal Data Protection and Information Commission is the competent supervisory authority for Transfers of Personal Information subject to FADP, and the UK's Information Commissioner's Office for Transfers of Personal Information subject to UK Data Protection Laws.

2.12.2 If the Services to be provided by Supplier requires the transfer of Personal Information of residents of the UK, and such transfer is subject to the laws of the UK (including the UK General Data Protection Regulation), the parties agree that:

- 2.12.2.1 The provisions of the UK 2021 SCCs Addendum shall apply in full. The official text of the UK 2021 SCCs Addendum is incorporated by reference.
- 2.12.2.2 For the purposes of Table 1 of the UK 2021 SCCs Addendum, the names of the parties, their roles and their details shall be set out in Attachment 1 in the attached [Appendix Annex I.A. of the 2021 SCCs]
- 2.12.2.3 For the purposes of Tables 2 and 3 of the UK 2021 SCCs Addendum, the version of the 2021 SCCs appended to this Exhibit, including the information set out in the Annexes of the 2021 SCCs, shall apply; and
- 2.12.2.4 For the purposes of Table 4 of the UK 2021 SCCs Addendum, neither party may end the UK 2021 SCCs Addendum.



2.12.2.5 Notwithstanding the foregoing, the UK 2021 SCCs Addendum will not apply to the extent the transfer is covered by an Adequacy Decision.

2.12.3 If Supplier is authorized by Buyer to subcontract any of its obligations under this Agreement, Supplier will downstream these obligations by entering into an appropriate onward transfer agreement, incorporating Module 3 of the 2021 EU SCCs (Processor-to-Processor) with any such subcontractor for any such disclosure.

2.12.4 If the European Commission or the United Kingdom updates, substitutes or modifies the relevant Standard Contractual Clauses, or if they are deemed invalid at any point during the term of this Agreement, then Supplier agrees to promptly execute such updated Standard Contractual Clauses or comply with such other cross-border data transfer mechanism deemed compliant by the relevant data protection authority(ies) in order to allow Personal Information to be transferred to Supplier and any affiliate or subcontractor of Supplier by Buyer or its affiliates.

**2.13 Supplier Compliance Cooperation.** Supplier shall take steps reasonably requested by Buyer to assist Buyer with respect to: (i) complying with or demonstrating Buyer's compliance with any notification, registration or other obligations applicable to Buyer or its affiliates under laws relating to Processing Personal Information under this Agreement; (ii) carrying out privacy and data protection impact assessments and related consultations by government authorities; (iii) demonstrating regulatory accountability; or (iv) ensuring the security of Personal Information. In the event this Agreement, or any actions to be taken or contemplated to be taken in performance of this Agreement, do not or would not satisfy either party's obligations under such laws, the parties shall cooperate with each other to execute an appropriate amendment to this Agreement.

**2.14 Security Controls.** Supplier shall (i) implement appropriate technical, physical, and organizational measures to ensure a level of security appropriate to the risk to Personal Information as required by all applicable Data Protection Laws, including measures in compliance with Buyer's Data Safeguard Exhibit XX; and (ii) impose a duty of strict confidentiality on any party authorized to access or Process Personal Information by or on behalf of Buyer.

**2.15 Third Party Beneficiaries.** Notwithstanding anything to the contrary in this Agreement, Buyer's affiliates are intended third-party beneficiaries of this Exhibit, shall be entitled to its benefits and shall be entitled to enforce this Exhibit as if each were a signatory hereto.

**2.16 Indemnification.** Supplier agrees to indemnify, defend and hold harmless Buyer and its affiliates and their directors, employees, and agents from and against any and all claims and resulting damages, liabilities, expenses, fines and losses of any type, to the extent arising out of, or relating to the following: (i) Supplier's failure (or the failure of any personnel, contractor, or agent of Supplier) to comply with the obligations under this Exhibit; (ii) any Privacy Breach; and (iii) any negligence or willful misconduct by Supplier, its personnel, contractor or agents or any third party to whom Supplier provides access to Personal Information Processed under this Agreement.

**2.17 Compliance with Law.** Supplier will comply with all applicable Data Protection Laws. Upon the reasonable request of Buyer, Supplier will promptly make available to Buyer all information in its possession necessary to demonstrate Supplier's compliance with its obligations under the applicable Data Protection Laws and the Agreement.

**2.18 Adverse Changes.** Supplier will notify Buyer in writing promptly, and no later than five (5) business days following such a determination, if Supplier: (i) has reason to believe that it is unable to comply with any of its obligations under this Agreement and it cannot cure this inability to comply within a reasonable timeframe; (ii) makes a determination that it can no longer meet its obligations under the Data Protection Laws; or (iii) becomes aware of any circumstances or change in applicable law that is likely to prevent it from fulfilling its obligations under this Agreement. Buyer has the right, upon providing notice to Supplier, to take reasonable and appropriate steps to stop and/or remediate unauthorized Processing of Personal Information, including where Supplier has notified Buyer that it can no longer meet its obligations under the Data Protection Laws. In the event that this Agreement or any actions to be taken or contemplated to be taken in performance of this Agreement, do not or

would not satisfy either party's obligations under the laws applicable to each party, the parties will negotiate in good faith upon an appropriate amendment to this Agreement.

**2.19 Conflicts.** To the extent there is any conflict between this Exhibit and the Agreement, the Exhibit will prevail. To the extent there is any conflict between this Exhibit and the terms of any applicable Model Contract, the terms of the Model Contract will prevail.

**2.20 Specific Jurisdictional Requirements.** The following provisions will apply to Personal Information in the specific countries set forth below:

(A) Argentina:

Where Buyer or a Buyer affiliate in Argentina transfers Personal Information to Supplier or any Supplier subcontractors located outside Argentina, such transfers shall be governed by the Argentine Model Clauses (Controller to Processor) set forth in Attachment 2 hereto, which are incorporated into this Exhibit and Agreements as if fully set forth herein. If the Argentine Model Clauses are applicable, then to the extent there is any conflict between the terms of this Exhibit and the terms of the Argentine Model Clauses, the Argentine Model Clauses shall control.

(B) Australia:

The following provisions apply solely if Buyer is located in Australia or Buyer otherwise notifies Supplier that this paragraph applies.

"Sensitive Information" is defined to include Personal Information about an individual's membership in a professional or trade association, in addition to the types of information identified in Section 1.12 of this Exhibit.

If Supplier uses or discloses Personal Information for one or more enforcement activities conducted by, or on behalf of, an enforcement body, Supplier must keep a written record of the use and disclosure and promptly provide a copy of the record to Buyer, unless such notice is prohibited by law applicable to Supplier.

Subject to Section 2.7 of this Exhibit, the Supplier "reasonably believes" that there has been a Privacy Breach, if at any time the Supplier has reasonable grounds to suspect that there has been a Privacy Breach.

The Supplier must comply with the Privacy Act 1988 (Cth) as amended from time to time, including the Australian Privacy Principles when dealing with Personal Information.

(C) China:

This Section applies solely if Buyer is located in China or Data Exporter otherwise notifies Supplier that this Section applies. Supplier must comply with the Cybersecurity and Personal Information Protection Laws in China, its implementing measures and other laws, regulations in relation to cybersecurity and data protection, especially to the extent inconsistent with the general stipulations in aforementioned sections under this Agreement including but not limited to definitions, sale of personal information and obligations concerned. "**Sensitive Personal Information**" is defined to include whereabouts and Personal Information of minors under the age of 14, in addition to the types of information identified in Section 1.12. Supplier shall agree to comply with the aforesaid applicable laws and regulations in China which may be promulgated, amended and updated from time to time unless there is an unforeseeable substantial obligation incurred by enforcing them. Under this circumstance, Supplier shall agree to negotiate with Buyer to come into an amendment of this Agreement to arrange the corresponding obligations.

(D) Indonesia:

The following provision applies solely if Buyer is located in Indonesia or Buyer otherwise notifies Supplier that this Section applies. If a Personal Data Breach occurs, Supplier will provide Buyer with information about the cause of the Personal Data Breach in the notice provided. Further, if the Personal Data Breach





poses potential harm to the individual, Supplier may request that Buyer confirm its receipt of the Personal Data Breach notification. All terms in this section to have the same meaning as they may be defined under applicable Data Protection Laws.

(E) Israel:

Supplier will keep databases containing Personal Information obtained from Buyer separate from information obtained from any other third party.

Without derogating from anything stated in this Exhibit or the associated Agreement, Supplier will comply with any and all obligations set out under the Protection of Privacy Regulations (Information Security) with respect to "holder" of a database, to the extent applicable.

(F) Japan:

The following provisions apply to Personal Information (a) Supplier receives or accesses from a Data Controller located in Japan; or (b) Buyer notifies Supplier is subject to these requirements.

F.1. Supplier may disclose or transfer such Personal Information to, or allow access to such Personal Information by (each, a "**Disclosure**"), a data processor that is not a party to this Agreement only if the following conditions are met: (1) Supplier has entered into a written agreement with the data processor that requires the data processor to undertake obligations at least as restrictive as the obligations undertaken by Supplier under this Agreement, including this Section F; and (2) Supplier reasonably supervises the Data Processor's overall compliance with the requirements in the written agreement executed under this Section F.1. A copy of the written agreement will be provided to Buyer promptly upon request. Supplier will remain liable to Buyer under this Agreement for all actions by the entity that receives information as a result of a Disclosure.

F.2. Supplier will be responsible for supervising all employees, contractors, subcontractors or agents that Supplier authorizes to Process such Personal Information with respect to their compliance with this Agreement.

F.3. Supplier will hold Personal Information in strict confidence and impose confidentiality obligations on personnel who will be provided access to or will otherwise Process Personal Information, including to protect all Personal Information consistent with the requirements of this Agreement (including during the term of their employment or engagement and thereafter).

F.4. Supplier will promptly notify Buyer, unless specifically prohibited by laws applicable to Supplier, if Supplier receives: (i) any requests from an individual with respect to Personal Information Processed, including but not limited to opt-out requests, requests for access and/or rectification, erasure, restriction, requests for data portability and all similar requests; or (ii) any complaint relating to Personal Information Processing, including allegations that the Processing infringes on an individual's rights. Supplier will not respond to any such request or complaint unless expressly authorized to do so by Buyer, will cooperate with Buyer with respect to any action taken relating to such request or complaint and will seek to implement appropriate processes (including technical and organizational measures) to assist Buyer in responding to requests or complaints from individuals.

F.5. Supplier will take any other steps reasonably requested by Buyer, and in particular to assist Buyer in meeting its obligations under Japanese Personal Information Protection Law, which include, but are not limited to (i) the notification and accountability to an individual, (ii) maintaining the security of the Personal Information, (iii) self-check as to whether Supplier has complied with this Agreement and reporting the result to Buyer at least once a year, and (iv) reporting as to whether or not there are local laws and/or regulations that would give negative impact on Supplier's compliance with this Agreement.

(G) Malaysia:

The following provisions apply to Personal Information (a) Supplier receives or accesses from a Data Controller located in Malaysia; or (b) Buyer notifies Supplier is subject to these requirements:



G.1. Only authorized staff can grant, modify or revoke access to information systems that use or houses Personal Information.

G.2. Supplier will maintain an audit log.

(H) Russia:

The following provisions apply to Personal Information (a) Supplier receives or accesses from a Data Controller located in Russia; or (b) Buyer notifies Supplier is subject to these requirements:

H.1.1. Supplier will maintain records specifying which media are used to store Personal Data.

H.1.2. Only authorized staff can grant, modify or revoke access to information systems that use or houses Personal Information.

H.1.3. Supplier will maintain an audit log.

H.2. Supplier's disaster recovery and business continuity plans will include processes to seek recovery of Personal Data that was modified or destroyed due to unauthorized access.

(I) South Africa:

For any contracts involving personal information of individuals of South Africa, the following terms and provisions will apply:

**"Anonymized Data"** means information that does not relate to an identified or identifiable individual or juristic person or Personal Information (as defined below) rendered anonymous in such a manner that the individual is not or is no longer identifiable.

**"Personal Information"** (or "Personal Data") means data that identifies, can be used to identify, relates to, or is capable of being associated with, or could reasonably be linked, directly or indirectly, with an individual or household, or juristic person, as defined by applicable law.

Supplier will treat data that identifies, can be used to identify, relates to, or is capable of being associated with, or could reasonably be linked, directly or indirectly, with a juristic person, the same as Personal Information.

Supplier will take reasonable measures to:

- identify all reasonably foreseeable internal and external risks to Personal Data
- establish and maintain appropriate safeguards against the risks identified
- regularly verify that the safeguards are effectively implemented
- ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards; and
- have due regard to generally accepted information security practices and procedures which may apply to that Party generally or be required in terms of specific industry or professional rules and regulations.

(J) South Korea:



Supplier will implement and maintain at least the specific technical and managerial safeguards as stipulated under the applicable laws including, but not limited to, the Personal Information Protection Act (“**PIPA**”), the Enforcement Decree of the PIPA and the Standards of Personal Information Security Measures.

Buyer may provide training to Supplier on a regular basis to ensure that Personal Information is not lost, stolen, leaked, altered, or damaged during the course of Processing such Personal Information and Supplier may not refuse such training.

Data Processor will be held liable for any and all actions or inactions by itself or its subcontractor with regard to the violation of this Agreement.



## ATTACHMENT 1

### EU STANDARD CONTRACTUAL CLAUSES

#### ANNEX

### STANDARD CONTRACTUAL CLAUSES

#### 1.

##### *Purpose and scope*

The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)<sup>1</sup> for the transfer of personal data to a third country.

The Parties:

the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and

the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”) have agreed to these standard contractual clauses (hereinafter: “Clauses”).

These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

##### *Effect and invariability of the Clauses*

These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

---

<sup>1</sup> Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.



These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

### ***Third-party beneficiaries***

Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);

Clause 9 - Clause 9(a), (c), (d) and (e);

Clause 12 - Clause 12(a), (d) and (f);

Clause 13;

Clause 15.1(c), (d) and (e);

Clause 16(e);

Clause 18 - Clause 18(a) and (b).

Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

### ***Interpretation***

Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

### ***Hierarchy***

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

### ***Description of the transfer(s)***

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.



### ***Docking clause***

An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

## **2. – OBLIGATIONS OF THE PARTIES**

### ***Data protection safeguards***

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

#### **1.1 Instructions**

The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

#### **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

#### **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

#### **Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.



### **Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

### **Security of processing**

The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

### **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter “sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.



## **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union<sup>2</sup> (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

## **Documentation and compliance**

The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

---

<sup>2</sup> The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union’s internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.



### *Use of sub-processors*

**GENERAL WRITTEN AUTHORISATION** The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least forty-five (45) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.<sup>3</sup> The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

### *Data subject rights*

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

---

<sup>3</sup> This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.



### ***Redress***

The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body<sup>4</sup> at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

refer the dispute to the competent courts within the meaning of Clause 18.

The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

### ***Liability***

(b) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

---

<sup>4</sup> The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.



The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

### *Supervision*

[Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

### **3. – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

#### *Local laws and practices affecting compliance with the Clauses*

The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.



The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

the laws and practices of the third country of destination— including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards<sup>5</sup>;

any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

---

<sup>5</sup> As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.



### *Obligations of the data importer in case of access by public authorities*

#### **Notification**

The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

#### **Review of legality and data minimisation**

The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

#### **4. – FINAL PROVISIONS**

##### ***Non-compliance with the Clauses and termination***

The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

the data importer is in substantial or persistent breach of these Clauses; or

the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

##### ***Governing law***

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Belgium.

##### ***Choice of forum and jurisdiction***

Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.



The Parties agree that those shall be the courts of Belgium.

A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

The Parties agree to submit themselves to the jurisdiction of such courts.

---



## APPENDIX

### ANNEX I

#### **A. LIST OF PARTIES**

##### **Data exporter(s):**

1. Name: Client.

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses: Activities relevant to the data transferred under these Clauses: Supplier will develop, edit and manage the art, layouts, & media materials for each brand ("Sales Aid Materials") for the various versions of the existing Canadian sales force HTML5 based sales app; assist with the upload of Sales Aid Materials into the sales app; and maintain the JJV Canada Dashboard (Dale).

Signature and date: See Agreement signature clauses.

Role (controller/processor): Controller

2. Any other Client that becomes party to the Agreement to which these Clauses are appended, including by entering into a Purchase Order or Statement of Work issued pursuant to such Agreement.

##### **Data importer(s):**

1. Name: Supplier1

Activities relevant to the data transferred under these Clauses: Supplier will develop, edit and manage the art, layouts, & media materials for each brand ("Sales Aid Materials") for the various versions of the existing Canadian sales force HTML5 based sales app; assist with the upload of Sales Aid Materials into the sales app; and maintain the JJV Canada Dashboard (Dale).

Signature and date: See Agreement signature clauses.

Role (controller/processor): processor

#### **B. DESCRIPTION OF TRANSFER**

*Categories of data subjects whose personal data is transferred*

- *Employees, former employees, contractors, agents, advisors, freelancers of the data exporter (who are natural persons)*



#### *Categories of personal data transferred*

- Personal identification information, such as first and last name
- Employer

*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

*None.*

The applied restrictions or safeguards are specified in Annex II

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*

*continuous*

*Nature of the processing*

- The nature of Processing of personal data by the data importer is for the performance of the Services pursuant to the Agreement.

*Purpose(s) of the data transfer and further processing*

- The purpose of Processing of personal data by the data importer is for the performance of the Services pursuant to the Agreement.

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

- Personal data will be retained for the term specified by the Agreement unless applicable law or legal preservation notice requires a longer retention period.

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

N/A

#### **C. COMPETENT SUPERVISORY AUTHORITY**

*Identify the competent supervisory authority/ies in accordance with Clause 13*

- Belgium - Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA).
- The supervisory authority/ies of any other J&J Affiliate in the European Economic Area that becomes a party (as data exporter) to the Agreement to which these Clauses are appended.

---

#### **ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

The technical and organisational measures are described in the Data Safeguards Exhibit of the Agreement to which these Clauses are attached.

---

#### **ANNEX III - LIST OF SUB-PROCESSORS**

The controller has authorised the use of the following sub-processors: N/A



**ATTACHMENT 2  
ARGENTINA  
(CONTROLLER TO PROCESSOR)**

**Contrato modelo de transferencia internacional de datos personales con motivo de prestación de servicios**

**Model Agreement of International Transfer of Personal Data for the case of Provision of Services**

Entre la entidad identificada en las páginas de firma de este contrato como el exportador de datos (en adelante, “el exportador de datos”) y la entidad identificada en las páginas de firma de este contrato como el importador de datos (en adelante, “el importador de datos”), en conjunto “las partes”, convienen el presente contrato de transferencia internacional de datos personales para la prestación de servicios, sometiéndola a los términos y condiciones que se detallan a continuación.

This International Transfer of Personal Data Agreement for the Provision of Services is entered into by and between the entity identified in the signature pages to this agreement as the data exporter (hereinafter the “data exporter”) and the entity identified in the signature pages to this agreement as the data importer (hereinafter the “data importer”), each a “party”, together “the parties,” pursuant to the terms and conditions provided hereafter.

**Cláusula 1) Definiciones**

**Clause 1 – Definitions**

A los efectos del presente contrato se entenderá por los siguientes términos:

For the purpose of this agreement, the following terms shall have their meaning assigned as follows:

a) “datos personales”, “datos sensibles”, “tratamiento”, “responsable” y “titular del dato”, el mismo significado que el establecido en la Ley N° 25.326, de Protección de Datos Personales.

a) “personal data,” “sensitive data,” “processing,” “responsible” and “data owner” shall have the meaning assigned in Act no. 25.326 of Protection of Personal Data.

b) “autoridad” o “autoridad de control”, la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES de la REPÚBLICA ARGENTINA.

b) “authority” or “supervisory authority” means the NATIONAL OFFICE FOR THE PROTECTION OF PERSONAL DATA in the REPUBLIC OF ARGENTINA.

c) “exportador”, el responsable del tratamiento que transfiera los datos personales;

c) “exporter” means the party responsible for processing who transfers the personal data;

d) “importador” o “encargado del tratamiento”, el prestador de servicios en los términos del artículo 25 de la Ley N° 25.326 radicado fuera de la jurisdicción argentina que reciba los datos personales procedentes del exportador de datos para su tratamiento de conformidad con los términos del presente.

d) “importer” or “processor” means the service provider in terms of Article 25 in Act no. 25.326 based outside Argentinean jurisdiction receiving the personal data from the exporter for their processing pursuant to the terms hereof.

e) por «legislación de protección de datos» se entenderá la Ley N° 25.326 y normativa reglamentaria.

e) “data protection legislation” means Act no. 25.326 and the regulations thereunder.



**Cláusula 2) Características, finalidad de la transferencia y términos específicos**

Los detalles y otros términos específicos de la transferencia y servicio previsto, como por ejemplo características de los datos personales transferidos, forma en que las partes pactan atender los pedidos del titular del dato o de la autoridad de control, transferencias previstas a terceros, y jurisdicción en que se radicarán los datos, se especifican en el Anexo A, que forma parte del presente contrato. Las partes podrán suscribir en el futuro anexos adicionales a fin de incorporar detalles y características de aquellas transferencias que se realicen con posterioridad y que se enmarquen en el presente contrato.

**Cláusula 3) Responsabilidad y terceros beneficiarios**

a) Los titulares de los datos, podrán exigir al Importador, en carácter de terceros beneficiarios, el cumplimiento de las disposiciones de la Ley N° 25.326 relacionadas con el tratamiento de sus datos personales, en particular lo relativo a los derechos de acceso, rectificación, supresión y demás derechos contenidos en el Capítulo III, artículos 13 a 20 de la Ley N° 25.326, conforme a las obligaciones y responsabilidades asumidas por las partes en el presente contrato; a tal fin, se someten a la jurisdicción argentina, tanto en sede judicial como administrativa. En aquellos casos en que se alegue incumplimiento por parte del importador de datos, el titular del dato podrá requerir al exportador que emprenda acciones apropiadas a fin de cesar dicho incumplimiento.

b) El importador acepta que la Autoridad de Control ejerza sus facultades respecto del tratamiento de datos que asume a su cargo, con los límites y facultades que le otorga la Ley N° 25.326, aceptando sus facultades de control y sanción, otorgándole a tales fines, en lo que resulte pertinente, el carácter de tercero beneficiario.

c) En caso que el Importador revoque, o no cumpla no obstante ser intimado por el Exportador otorgando un plazo perentorio de CINCO (5) días hábiles, con los derechos y facultades reconocidos a terceros beneficiarios en esta cláusula, tal hecho será causal de resolución automática del presente Contrato.

**Clause 2 – Characteristics, Purpose of the Transfer and Specific Terms**

The details and other specific terms of the transfer and the service to be provided, including the characteristics of the transferred personal data, the manner in which the parties agree to address the requests from the data owner or the supervisory authority, any third-party transfers foreseen, and the jurisdiction where the data shall be stored, are detailed in Annex A, which is an integral part of this agreement. The parties may agree in the future on additional annexes in order to include details and characteristics of any subsequent transfers and subject them to this agreement.

**Clause 3 – Liability and Third-Party Beneficiaries**

a) Data owners may require the importer, in their capacity as third-party beneficiaries, to comply with the provisions in Act no. 25.326 in relation to the processing of their personal data, in particular relating to the rights of access, correction, suppression and other rights contained in Chapter III, Articles 13 to 20 in Act no. 25.326, in accordance with the obligations and responsibilities undertaken by the parties in this agreement; to that end, they submit to Argentinean jurisdiction, in terms of both judicial and administrative venue. In such cases where non-compliance by the data importer is alleged, the data owner may require the exporter to take appropriate actions in order to cease such non-compliance.

b) The importer accepts that the Supervisory Authority may exercise its powers regarding the processing of data undertaken by the importer, with the limits and powers granted by Act no. 25.326, accepting their supervision and sanction authorities, granting them for such purposes, as applicable, the capacity of third-party beneficiary.

c) In case the importer refuses, or fails to comply in spite of the exporter's requirement setting a deadline of FIVE (5) working days, with the rights and powers recognized in this clause to be given third-party beneficiaries, such event shall be a cause for automatic termination of this agreement.





d) Los titulares de los datos podrán exigir al importador el cumplimiento de obligaciones asumidas en el presente contrato relativas al tratamiento de los datos que sean propias del exportador, cuando este último haya desaparecido de hecho o haya cesado de existir jurídicamente, a menos que cualquier entidad sucesora haya asumido la totalidad de las obligaciones jurídicas del exportador de datos en virtud de contrato o por ministerio de la ley, en cuyo caso los titulares de los datos podrán exigirlos a dicha entidad.

d) Data owners may require the importer to comply with the obligations undertaken by the data exporter in this agreement in relation to the data processing, in case the data exporter has disappeared in fact or has ceased to exist legally, unless a successor entity has undertaken all the legal obligations of the data exporter via an agreement or by law, in which case data owners may require such compliance from such entity.

e) Los titulares de los datos podrán exigir al eventual subencargado de tratamiento de datos el cumplimiento de la presente cláusula y el cumplimiento de obligaciones asumidas en el presente contrato por parte del exportador y el importador, relativas al tratamiento de los datos que sean propias del exportador, cuando ambos hayan desaparecido de facto o hayan cesado de existir jurídicamente, a menos que cualquier entidad sucesora haya asumido la totalidad de las obligaciones jurídicas de alguno de ellos en virtud de contrato o por ministerio de la ley, en cuyo caso los titulares de los datos podrán exigirlos a dicha entidad. La responsabilidad civil del subencargado del tratamiento de datos se limitará a sus propias operaciones de tratamiento de datos según lo pactado entre las partes y estas cláusulas.

e) Data owners may require any ultimate sub-processor to comply with this clause and with the obligations undertaken by the data exporter and the data importer in this agreement in relation to the processing of data that belong to the exporter, in case both have disappeared in fact or have ceased to exist legally, unless a successor entity has undertaken all the legal obligations of either of them via an agreement or by law, in which case data owners may require such compliance from such entity. The liability of the sub-processor shall be limited to its own data processing operations as agreed upon by the parties and these clauses.

f) Las partes no se oponen a que los titulares de los datos estén representados por una asociación u otras entidades previstas por la ley Argentina.

f) The parties have no objection against the data owners being represented by an association or other entities foreseen in Argentinean law.

#### **Cláusula 4) Obligaciones del exportador de datos**

#### **Clause 4 – Data Exporter Obligations**

El exportador de datos acuerda y garantiza lo siguiente:

The data exporter agrees and warrants the following:

a) La recopilación, el tratamiento y la transferencia de los datos personales se han efectuado y efectuarán de conformidad con la Ley N° 25.326.

a) The collection, processing and transfer of personal data have been and shall be made pursuant to Act no. 25.326.

b) Ha realizado esfuerzos razonables para determinar si el importador de datos es capaz de cumplir las obligaciones pactadas en el presente contrato. A tal efecto, el exportador podrá solicitar al importador la contratación de un seguro de responsabilidad para eventuales perjuicios ocasionados con motivo del tratamiento previsto, conforme se especifica en el Anexo A.

b) The exporter has made reasonable efforts to determine whether the data importer is capable of complying with the obligations in this agreement. To that aim, the exporter may request that the importer obtain liability insurance for potential damages arising from the foreseen processing, as specified in Annex A.



c) Durante la prestación de los servicios de tratamiento de los datos personales, dará las instrucciones necesarias para que el tratamiento de los datos personales transferidos se lleve a cabo exclusivamente en su nombre y de conformidad con la Ley N° 25.326 y el presente contrato;

d) Hará entrega al importador de copia de la legislación vigente en Argentina aplicable al tratamiento de datos previsto.

e) Garantiza que ha cumplido en informar a los titulares de los datos que su información personal podía ser transferida a un tercer país con niveles inferiores de protección de datos a los de la REPÚBLICA ARGENTINA;

f) Garantiza que en caso de subtratamiento la actividad se llevará a cabo por un subencargado que deberá contar con su conformidad previa expresa del exportador y que proporcionará por lo menos el mismo nivel de protección de los datos personales y derechos de los titulares de los datos que los aquí pactados con el importador de datos, celebrando un contrato a tales fines, y quien estará también bajo las instrucciones del Exportador;

g) En caso de ejercicio por parte del titular de los datos —como tercero beneficiario— de sus derechos de acceso, rectificación, supresión y demás derechos contenidos en el Capítulo III, artículos 13 a 20 de la Ley N° 25.326, dará respuesta al mismo dentro de los DIEZ (10) días corridos si se refiere a un pedido de acceso y de CINCO (5) días hábiles si se refiere a un pedido de rectificación, supresión o actualización, y disponiendo los medios para tal fin, sea por los datos en su poder o por haberse pactado como obligación a su cargo, lo que se indica en el Anexo A. Responderá en los plazos dispuestos por la Ley N° 25.326 las consultas de los titulares de los datos y de la autoridad relativas al tratamiento de los datos personales por parte del importador, a menos que las partes hayan acordado que sea el importador quien responda a estas consultas. Aun en este supuesto, será el exportador quien deba responder, en la medida de lo razonablemente posible y a partir de la información de que razonablemente pueda disponer, si el importador de datos es incapaz de responder o no lo realiza.

c) During the provision of personal data processing services, the data exporter shall provide the instructions necessary for the processing of the transferred personal data to be carried out exclusively on the exporter's behalf and in accordance with Act no. 25.326 and this Agreement.

d) The data exporter shall provide the importer with a copy of the current legislation in Argentina applicable to the foreseen data processing.

e) The data exporter warrants it has complied with informing the data owners that their personal information might be transferred to a third country with levels of data protection lower than those in the REPUBLIC OF ARGENTINA.

f) The data exporter warrants that in case of sub-processing, such activity shall be conducted by a sub-processor that must have prior express approval of the exporter and which shall provide at least the same level of protection of personal data and of the rights of data owners as the level agreed-to herein with the data importer, entering an agreement for such purpose, and the sub-processor shall also be under the instructions of the data exporter.

g) In the event that a data owner—acting as beneficiary third-party—exercises its rights of access, correction, suppression and other rights contained in Chapter III, Articles 13 to 20 in Act no. 25.326, the data exporter shall reply within TEN (10) calendar days in case of a request for access and within FIVE (5) working days in case of a request for correction, suppression or update, and by making available the means for such purpose, whether for the data in its possession or as agreed to be its obligation, as provided in Annex A. The exporter shall respond to the queries from the data owner and the authority in relation to the processing of the personal data by the importer within the time periods laid down in Act no. 25.326, unless the parties have agreed that it shall fall upon the importer to respond to such queries. Even in the latter scenario, it shall be the exporter who shall respond, as far as reasonably possible and based on the information it may reasonably have available, should the data importer be unable or fail to respond.



h) Pondrá a disposición de los titulares de los datos, en su carácter de terceros beneficiarios a tenor de la cláusula 3, y a petición de éstos, una copia de las cláusulas que se relacionen al tratamiento de sus datos personales, derechos y garantías, así como una copia de las cláusulas de otros contratos necesarios para los servicios de subtratamiento de los datos que deba efectuarse de conformidad con este contrato.

h) The exporter shall make available to data owners, in their capacity as third-party beneficiaries under Clause 3, and at their request, a copy of the clauses relating to the processing of their personal data, their rights and guarantees, as well as a copy of any other agreement for the data sub-processing services required to be entered in accordance this Agreement.

#### **Cláusula 5) Obligaciones del importador de datos**

#### **Clause 5 – Data Importer Obligations**

El importador de datos acuerda y garantiza lo siguiente:

The data importer agrees and warrants the following:

a) tratará los datos personales transferidos solo en nombre del exportador de datos, de conformidad con sus instrucciones y las cláusulas. En caso de que no pueda cumplir estos requisitos por la razón que fuere, informará de ello sin demora al exportador de datos, en cuyo caso este estará facultado para suspender la transferencia de los datos o rescindir el contrato;

a) The data importer shall process the transferred personal data only on behalf of the data exporter, in accordance with its instructions and the Agreement. Should the data importer be unable to comply with these requirements for any reason, the data importer shall notify the data exporter without delay, and the data exporter shall be entitled in this case to suspend the data transfer or to terminate the Agreement.

b) disponer las medidas de seguridad y confidencialidad necesarias y efectivas para evitar la adulteración, pérdida, consulta o tratamiento no autorizado de los datos, y que permitan detectar desviaciones, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado verificando que no sean inferiores a las dispuestas por la normativa vigente, de manera tal que garanticen el nivel de seguridad apropiado a los riesgos que entraña el tratamiento y a la naturaleza de los datos que han de protegerse;

b) The importer has in place security and confidentiality measures that are necessary and effective to avoid any altering, loss, unauthorized access or processing of data and that allow it to detect deviations, whether intentional or not, whether the risks arise from human actions or from the technical means employed, verifying that they are no less stringent than provided for by current law, in order to ensure an appropriate level of security from the risks involved in the processing and the nature of the data to be protected.

c) dispondrá de procedimientos que garanticen que todo acceso a los datos transferidos se realizará por personal autorizado para ello, estableciendo niveles de acceso y claves, quienes cumplirán con el deber de confidencialidad y seguridad de los mismos, suscribiendo convenios a tales fines.

c) The importer shall have procedures in place, ensuring that any access to the transferred data is made by staff authorized for such purpose, establishing access levels and controls, who shall comply with the confidentiality and security obligations in relation thereto by signing agreements for such purpose.

d) que ha verificado que la legislación local no impide el cumplimiento de las obligaciones, garantías y principios previstos en el presente contrato relativos al tratamiento de los datos personales y sus titulares, e informará al exportador de datos en forma inmediata en caso de tener conocimiento de la existencia de alguna

d) The importer has verified that local legislation does not prevent the fulfillment of the obligations, warranties and principles foreseen in this agreement in relation to the processing of personal data and their owners, and shall immediately notify the data exporter if he becomes aware of the



disposición de esta índole, en cuyo caso el Exportador podrá suspender la transferencia;

existence of any such provision, in which case the exporter may suspend the transfer.

e) tratará los datos personales siguiendo las expresas instrucciones que le imparta el exportador conforme a los fines y forma descriptos en el Anexo A;

e) The data importer shall process the personal data following the express instructions from the exporter in accordance with the purposes and manner set forth in Annex A.

f) comunicará al exportador de datos un punto de contacto dentro de su organización autorizado a responder a las consultas que guarden relación con el tratamiento de datos personales y cooperará de buena fe con el exportador de datos, el titular del dato y la autoridad respecto de tales consultas dentro de los plazos de ley. En caso de que el exportador de datos haya cesado de existir jurídicamente, o si así lo hubieran acordado las partes, el importador de datos asumirá las tareas relativas a su cumplimiento conforme a lo dispuesto en la letra d) de la cláusula 3;

f) The importer shall communicate to the data exporter a contact person within its organization authorized to reply to queries in relation to the processing of personal data and shall cooperate in good faith with the data exporter, the data owners and the authority in connection with such queries within the legal time periods. In case the data exporter ceases to exist legally, or if so agreed by the parties, the data importer shall undertake the tasks related to its compliance per the provisions of item (d) in Clause 3.

g) pondrá a disposición, a solicitud del exportador de datos o la autoridad, sus instalaciones de tratamiento de datos, sus ficheros y toda la documentación necesaria para el tratamiento, a efectos de revisión, auditoría o certificación. Estas labores serán realizadas, previa notificación razonable y durante horas laborables normales, por un inspector o auditor imparcial e independiente designados por el exportador o la autoridad, a fin de determinar si se cumplen las garantías y los compromisos previstos en el presente contrato;

g) The importer shall make available, at the request of the data exporter or the authority, its data processing facilities, files and any other documentation as may be necessary for the processing activities, for the purposes of review, audit or certification. These activities shall be conducted, with reasonable prior notification and during regular working hours, by an impartial and independent inspector or auditor appointed by the exporter or the authority, with the aim of determining whether the warranties and commitments laid down in this agreement are being met.

h) tratará los datos personales de conformidad con la Ley N° 25.326, de protección de datos personales;

h) The importer shall process the personal data in accordance with Act no. 25.326 on personal data protection.

i) notificará sin demora al exportador de datos sobre: i) toda solicitud jurídicamente vinculante de ceder datos personales presentada por una autoridad encargada de la aplicación de ley a menos que esté prohibido por la normativa aplicable (en la medida que no excedan lo necesario en una sociedad democrática siguiendo las pautas del epígrafe siguiente, punto 2), ii) todo acceso accidental o no autorizado, iii) toda solicitud sin respuesta recibida directamente de los titulares de los datos, a menos que se le autorice;

i) The importer shall notify the data exporter without delay about: (i) any legally binding request to produce personal data presented by a law enforcement authority, unless it is prohibited by the applicable law (to the extent this does not exceed what is required in a democratic society following the guidelines in the next paragraph, item 2); (ii) any accidental or unauthorized access; (iii) any request from the data owners without responding, unless authorized.

j) no cederá ni transferirá los datos personales a terceros excepto que: 1) se establezca de manera específica en el Anexo A del presente contrato o

j) The importer shall not assign or transfer personal data to any third party, unless: (1) it is specifically provided in Annex A to this agreement or



resulte necesario para su cumplimiento, verificando en ambos casos que el destinatario se obligue en iguales términos que el importador en el presente y siempre con el conocimiento y conformidad previa del exportador, o 2) la cesión sea requerida por ley o autoridad competente, en la medida que no exceda lo necesario en una sociedad democrática, por ejemplo, cuando constituya una medida necesaria para la salvaguardia de la seguridad del Estado, la defensa, la seguridad pública, la prevención, la investigación, la detección y la represión de infracciones penales o administrativas, o la protección del titular del dato o de los derechos y libertades de otras personas.

Al recibir la solicitud señalada arriba como punto 2), el Importador deberá de manera inmediata: a) verificar que la autoridad solicitante ofrezca garantías adecuadas de cumplimiento de los principios del artículo 4° de la Ley N° 25.326, y de los derechos de los titulares de los datos para el acceso, rectificación, supresión y demás derechos contenidos en el Capítulo III, artículos 13 a 20 de la Ley N° 25.326 salvo en los siguientes casos y condiciones (conforme artículo 17 de la Ley N° 25.326): i) previstos por la ley o mediante decisión fundada en la protección de la defensa de la Nación, el orden y la seguridad públicos, o la protección de los derechos e intereses de terceros, ii) mediante resolución fundada y notificada al afectado, cuando pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones sujetas a control estatal y relativas al orden público, como ser: tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas; sin perjuicio de ello, se deberá brindar el acceso a los datos en la oportunidad en que el afectado tenga que ejercer su derecho de defensa; y b) en caso que la autoridad no otorgue u ofrezca las garantías indicadas en el punto a) inmediato anterior, prevalecerá la ley argentina, por lo que el Importador procederá a suspender el tratamiento en dicho país reintegrando los datos al Exportador según las instrucciones que este le imparta y notificando este último a la autoridad de control.

k) atenderá los pedidos que reciba del titular del dato como tercero beneficiario, o del exportador, con motivo del ejercicio de los derechos de acceso, rectificación, supresión y demás derechos

necessary for compliance therewith, verifying in both cases that the recipient is bound by equivalent terms as the importer herein and in any case with the exporter's prior knowledge and acceptance; or (2) the assignment is required by law or by a competent authority, to the extent it does not exceed what is required in a democratic society, for instance, when it is a measure necessary to safeguard the State's security, defense, public security, the prevention, investigation, detection and repression of criminal or administrative offenses, or the protection of the data owner or the rights or liberties of other persons.

Upon the receipt of the request per (2) above, the importer shall immediately: (a) verify that the requesting authority offers adequate guarantees of compliance with the principles of Article 4 in Act no. 25.326 and of the data owners' rights of access, correction, suppression and other rights contained in Chapter III, Articles 13 to 20 in Act no. 25.326, except in the cases and conditions hereafter (per Article 17 in Act no. 25.326): (i) foreseen by law or by a judgment on the grounds of the protection of the Nation's defense, public order and security, or the protection of third-party rights and interests; (ii) by means of a resolution founded and notified to the interested party, when they could obstruct ongoing judicial or administrative proceedings linked to the investigation of compliance with obligations subject to state control and in relation to public order, such as tax or social security, the performance of health and environment control duties, the investigation of criminal offenses and the verification of administrative infringements; without prejudice to the above, access to the data shall be granted when the affected party must exercise its right to defense; and (b) in case the authority does not provide or offer the guarantees set out in the preceding (a), Argentinean law shall prevail, therefore the importer shall proceed to suspend the processing activities in such country, returning the data to the exporter per the exporter's instructions, who shall notify the supervisory authority.

k) The importer shall address the requests from the data owner as a third-party beneficiary, or from the exporter, to exercise the rights of access, correction, suppression and others contained in





contenidos en el Capítulo III, artículos 13 a 20 de la Ley N° 25.326, respetando los plazos de ley y disponiendo los medios para tal fin. Responderá en los plazos dispuestos por la Ley N° 25.326 las consultas de los titulares de los datos y de la autoridad relativas al tratamiento de los datos personales por parte del importador de datos, sin perjuicio que las partes hayan acordado de otra forma quien responda a estas consultas en el Anexo A, siguiendo las instrucciones de la autoridad de control;

Chapter III, Articles 13 to 20 in Act no. 25.326, observing the legal time periods and making available the means to such end. The importer shall respond to the queries from the data owner and the authority in relation to the processing of the personal data by the importer within the time periods laid down in Act no. 25.326, without prejudice to the parties having agreed otherwise on who must respond to these queries in Annex A, following the directions from the supervisory authority.

l) destruirá, certificando tal hecho, y/o reintegrará al exportador los datos personales objeto de la transferencia, cuando por cualquier causa se resuelva el presente Contrato.

l) The importer shall destroy, providing the relevant certification, and/or return to the exporter the personal data subject to transfer, in case of termination of this Agreement for any cause.

ll) que, en caso de subtratamiento de los datos, habrá informado previamente al exportador de datos y obtenido previamente su consentimiento por escrito;

m) In case of data sub-processing, the importer shall previously inform the data exporter and obtain its approval in writing.

m) que los servicios de tratamiento por el eventual subencargado del tratamiento se llevarán a cabo de conformidad con la cláusula específica N° 10;

n) The processing services by any eventual sub-processor shall be conducted in accordance with the specific Clause 10.

n) enviará sin demora al exportador de datos una copia del contrato que celebre con el subencargado del tratamiento con arreglo a este contrato y en el que se ha de otorgar al Exportador el carácter de tercero beneficiario a fin de impartir las instrucciones que considere necesarias y facultades para resolverlo.

o) The importer shall submit to the data exporter a copy of any agreement entered into with a sub-processor in accordance with this agreement, and in such agreement the exporter shall be designated a third-party beneficiary for the purpose of giving any instructions as it deems necessary, as well as powers to terminate such agreement.

ñ) llevará registro del cumplimiento de las obligaciones asumidas en la presente cláusula, cuyo informe estará disponible a pedido del exportador o la autoridad.

p) The importer shall keep a record of compliance with the obligations contained in this clause, the report of which shall be made available at the request of the exporter or the authority.

## **Cláusula 6) Responsabilidad**

## **Clause 6 – Liability**

a) Las partes acuerdan que los titulares de los datos que hayan sufrido daños como resultado del incumplimiento de las obligaciones pactadas en el presente Contrato por cualquier parte o subencargado del tratamiento, tendrán derecho a percibir una indemnización del exportador de datos para reparar el daño sufrido.

a) The parties agree that data owners suffering any damage arising from non-compliance with the obligations set forth in this agreement by any party or sub-processor shall be entitled to indemnification from the data exporter to remedy the damage suffered.

b) En caso que el titular del dato no pueda interponer contra el exportador de datos la demanda de indemnización a que se refiere el epígrafe 1 por incumplimiento por parte del

b) In the event that a data owner is unable to demand indemnification from the data exporter per epigraph 1) for the data importer's or its sub-processor's failure to comply with their obligations



importador de datos o su subencargado de sus obligaciones impuestas en las cláusulas 5 y 10, por haber desaparecido de facto, cesado de existir jurídicamente o ser insolvente, el importador de datos acepta que el titular del dato pueda demandarle a él en el lugar del exportador de datos, a menos que cualquier entidad sucesora haya asumido la totalidad de las obligaciones jurídicas del exportador de datos en virtud de contrato o por ministerio de la ley, en cuyo caso los titulares de los datos podrán exigir sus derechos a dicha entidad. El importador de datos no podrá basarse en un incumplimiento de un subencargado del tratamiento de sus obligaciones para eludir sus propias responsabilidades.

c) En caso de que el titular del dato no pueda interponer contra el exportador de datos o el importador de datos la demanda a que se refieren los apartados 1 y 2, por incumplimiento por parte del subencargado del tratamiento de datos de sus obligaciones impuestas en la cláusula 3 o en la cláusula 10, por haber desaparecido de facto, cesado de existir jurídicamente o ser insolventes ambos, tanto el exportador de datos como el importador de datos, el subencargado del tratamiento de datos acepta que el titular del dato pueda demandarle a él en cuanto a sus propias operaciones de tratamiento de datos en virtud de las cláusulas en el lugar del exportador de datos o del importador de datos, a menos que cualquier entidad sucesora haya asumido la totalidad de las obligaciones jurídicas del exportador de datos o del importador de datos en virtud de contrato o por ministerio de la ley, en cuyo caso los titulares de los datos podrán exigir sus derechos a dicha entidad. La responsabilidad del subencargado del tratamiento se limitará a sus propias operaciones de tratamiento de datos con arreglo a las presentes cláusulas.

imposed in Clauses 5 and 10, due to the fact that the exporter has disappeared in fact, ceased to exist legally or gone into bankruptcy, the data importer agrees that the data owner may make a demand against the importer in lieu of the data exporter, unless a successor entity has undertaken all the legal obligations of the data exporter via contract or by law, in which case data owners may require such compliance from such entity. The data importer shall not evade its own liability on the grounds of any sub-processor's non-compliance with its obligations.

c) In the event that a data owner is unable to make the demand referenced in epigraphs 1) and 2) above against the data exporter or the data importer, for non-compliance by the sub-processor with its obligations imposed in Clauses 3 or 10, due to the fact that both the data importer and the data exporter have disappeared in fact, ceased to exist legally or gone into bankruptcy, the sub-processor agrees that the data owner may make a demand against the sub-processor in relation to its own data processing operations under the agreement in lieu of the data exporter or the data importer, unless a successor entity has undertaken all the legal obligations of the data exporter or the data importer via contract or by law, in which case data owners may require such compliance from such entity. The liability of the sub-processor shall be limited to its own data processing operations in accordance with this agreement.

#### **Cláusula 7) Legislación aplicable y jurisdicción**

El presente contrato se regirá por la ley de la REPÚBLICA ARGENTINA, en particular la Ley N° 25.326, sus normas reglamentarias y disposiciones de la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES, y entenderán en caso de conflicto vinculado a la protección de datos personales la jurisdicción judicial y administrativa de la REPÚBLICA ARGENTINA.

#### **Clause 7 – Governing Law and Jurisdiction**

This Agreement shall be governed by the law of the REPUBLIC OF ARGENTINA, in particular Act no. 25.326, the regulations thereunder and the provisions of the NATIONAL OFFICE FOR THE PROTECTION OF PERSONAL DATA, and in case of conflict in relation to the protection of personal data, shall be subject to judicial and administrative jurisdiction of the REPUBLIC OF ARGENTINA.





**Cláusula 8) Resolución de conflictos con los titulares de los datos**

a) El importador de datos acuerda que si el titular del dato invoca en su contra derechos de tercero beneficiario o reclama una indemnización por daños y perjuicios con arreglo a las cláusulas, aceptará la decisión del titular del dato de: i) someter el conflicto a mediación por parte de una persona independiente; ii) presentar denuncia ante la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES; y iii) someter el conflicto a los tribunales argentinos competentes.

b) Las partes acuerdan que las opciones del titular del dato no obstaculizarán sus derechos sustantivos o procedimentales a obtener reparación de conformidad con otras disposiciones de Derecho nacional o internacional.

**Cláusula 9) Cooperación con las autoridades de control**

a) Las partes acuerdan que la autoridad de control está facultada para auditar al importador, o a cualquier subencargado, en la misma medida y condiciones en que lo haría respecto del exportador de datos conforme a la Ley N° 25.326, poniendo a disposición sus instalaciones de tratamiento de los datos. Las tareas de auditoría podrán ser realizadas tanto por personal de la autoridad de control como por terceras personas idóneas por ella designadas para dicho acto o autoridades locales de competencias análogas en colaboración con la autoridad.

b) El importador de datos informará sin demora al exportador de datos en el caso de que la legislación existente aplicable a él o a cualquier subencargado no permita auditar al importador ni a los subencargados.

**Cláusula 10) Subtratamiento de datos**

a) El importador de datos no subcontratará ninguna de sus operaciones de procesamiento llevadas a cabo en nombre del exportador de datos con arreglo a las cláusulas sin previo consentimiento por escrito del exportador de datos. Si el importador de datos subcontrata sus obligaciones deberá realizarse mediante un acuerdo escrito en el que el subencargado asuma iguales obligaciones que el importador, en lo que resulte compatible, sea frente al exportador de

**Clause 8 – Resolution of Conflicts with Data Owners**

a) The data importer agrees that if a data owner exercises against the importer its rights as a third party beneficiary or demands indemnification for damages pursuant to these clauses, the data importer shall abide the data owner's decision to: (i) submit the conflict to mediation by an independent party; (ii) file a complaint with the NATIONAL OFFICE FOR THE PROTECTION OF PERSONAL DATA; and (iii) submit the conflict to the competent Argentinean court.

b) The parties agree that the data owner's choices shall not affect its substantive or procedural rights to seek relief in accordance with other provisions of national or international law.

**Clause 9 – Cooperation with Supervisory Authorities**

a) The parties agree that the supervisory authority is entitled to audit the importer or any sub-processor, to the same extent and under the same conditions as they would audit the data exporter pursuant to Act no. 25.326, making available their data processing facilities. Auditing activities may be conducted both by supervisory authority personnel and by suitable third persons appointed thereby for such purposes, or by local authorities of similar competencies in collaboration with the authority.

b) The data importer shall notify the data exporter without delay in case the existing legislation applicable to the importer or to any of its sub-processors does not allow auditing of the importer or its sub-processors.

**Clause 10 – Data Sub-processing**

a) The data importer shall not subcontract any of its processing operations conducted on behalf of the data exporter pursuant to this agreement without prior approval in writing from the data exporter. Should the data importer subcontract its obligations, it shall be by means of an agreement in writing where the sub-processor undertakes obligations equivalent to those of the importer, where compatible, either towards the data exporter or towards the data owner and the supervisory



datos como el titular del dato y la autoridad de control, como terceros beneficiarios. En los casos en que el subencargado del tratamiento de datos no pueda cumplir sus obligaciones de protección de los datos con arreglo a dicho acuerdo escrito, el importador de datos seguirá siendo plenamente responsable frente al exportador de datos del cumplimiento de las obligaciones del subencargado del tratamiento de datos con arreglo a dicho acuerdo.

b) El contrato escrito previo entre el importador de datos y el subencargado del tratamiento contendrá asimismo una cláusula de tercero beneficiario que incluya aquellos casos en que el titular del dato no pueda interponer la demanda de indemnización a que se refiere el apartado a) de la cláusula 6 contra el exportador de datos o el importador de datos por haber estos desaparecido de facto, cesado de existir jurídicamente o ser insolventes, y ninguna entidad sucesora haya asumido la totalidad de las obligaciones jurídicas del exportador de datos o del importador de datos en virtud de contrato o por ministerio de la ley. Dicha responsabilidad civil del subencargado del tratamiento se limitará a sus propias operaciones de tratamiento de datos conforme tareas subcontratadas.

c) Las disposiciones sobre aspectos de la protección de los datos en caso de subcontratación de operaciones de procesamiento se regirán por la legislación Argentina. Este requisito puede verse satisfecho mediante contrato entre importador y subencargado en el cual este último es cosignatario del presente Contrato.

d) El exportador de datos conservará la lista de los acuerdos de subtratamiento celebrados por el importador de datos, lista que se actualizará al menos una vez al año. La lista estará a disposición de la autoridad de control.

#### **Cláusula 11) Resolución del Contrato**

a) En caso que el importador de datos incumpla las obligaciones que le incumben en virtud de las presentes cláusulas, el exportador de datos deberá suspender temporalmente la transferencia de datos personales al importador hasta que se subsane el incumplimiento en plazo perentorio que le fije según la gravedad del hecho, notificando de dicho hecho a la autoridad de control.

authority, as third-party beneficiaries. In case the sub-processor is unable to comply with its data protection obligations pursuant to such written agreement, the data importer shall remain fully liable to the data exporter for the sub-processor's compliance with its obligations in accordance with this agreement.

b) The above-mentioned written agreement between the data importer and the sub-processor shall also contain a third-party beneficiary clause including such cases where the data owner is unable to demand the indemnity referenced in Clause 6 item (a) against the data importer or the data exporter due to their having disappeared in fact, ceased to exist legally or gone into bankruptcy, and no successor entity has undertaken all of the legal obligations of the data exporter or the data importer via contract or by law. Such liability of the sub-processor shall be limited to its own data processing operations according to the subcontracted activities.

c) The provisions on data protection issues in case of the subcontracting of processing operations shall be governed by Argentinean law. This requirement may be met through an agreement between the importer and the sub-processor where the latter is included as a co-signer of this agreement.

d) The data exporter shall preserve the list of sub-processing agreements entered into by the data importer, which shall be updated at least once per year. Such list shall be available to the supervisory authority.

#### **Clause 11 – Termination of the Contract**

a) In case the data importer fails to comply with its obligations under these clauses, the data exporter shall temporarily suspend the transfer of personal data to the importer until the non-compliance is remedied within the deadline fixed according to the severity of the circumstance, notifying the supervisory authority about this.



b) El contrato se tendrá por resuelto, y así deberá declararlo el exportador previa intervención de la autoridad de control, en caso de que: i) la transferencia de datos personales al importador de datos haya sido suspendida temporalmente por el exportador de datos durante un período de tiempo superior a TREINTA (30) días corridos de conformidad con lo dispuesto en la letra a); ii) el cumplimiento por parte del importador de datos del presente contrato y la ley aplicable sean contrarios a disposiciones legales o reglamentarias en el país de importación; iii) el importador de datos incumpla de forma sustancial o persistente cualquier garantía o compromiso previstos en las presentes cláusulas; iv) una decisión definitiva y firme, contra la que no pueda entablarse recurso alguno de un tribunal argentino o de la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES, que establezca que el importador o el exportador de datos han incumplido el Contrato; o v) El exportador de datos, sin perjuicio del ejercicio de cualquier otro derecho que le pueda asistir contra el importador de datos, podrá resolver las presentes cláusulas cuando: se haya solicitado la administración judicial o la liquidación del importador de datos y dicha solicitud no haya sido desestimada en el plazo previsto al efecto con arreglo a la legislación aplicable; se emita una orden de liquidación o se decrete su quiebra; se designe a un administrador de cualquiera de sus activos; el importador de datos haya solicitado la declaración de concurso de acreedores; o se encuentre en una situación análoga ante cualquier jurisdicción. En los casos contemplados en los incisos i), ii), o iv), también podrá proceder a la resolución el importador de datos sin necesidad de intervención de la autoridad de control.

c) Las partes acuerdan que la resolución del presente contrato por motivo que fuere no las eximirá del cumplimiento de las obligaciones y condiciones relativas al tratamiento de los datos personales transferidos.

**Cláusula 12) Obligaciones una vez finalizada la prestación de los servicios de tratamiento de los datos personales**

Las partes acuerdan que, una vez finalizada la prestación de los servicios de tratamiento de los datos personales, por motivo que fuere, el importador y el subencargado deberán, a discreción del exportador, o bien devolver todos los datos personales transferidos y sus copias, o bien

b) The Agreement shall be deemed terminated, and the exporter shall declare it as such pending the intervention of the supervisory authority, in the event that (i) the transfer of personal data to the importer has been temporarily suspended by the data exporter during a period exceeding THIRTY (30) calendar days as described in (a) above; (ii) the compliance by the data importer with this Agreement and the applicable law is contrary to legal or regulatory provisions in the country of import; (iii) the data importer fails to comply substantially or persistently with any guarantee or commitment foreseen in these clauses; (iv) a final and firm judgment, against which no further appeal is possible, is issued by an Argentinean court or by the NATIONAL OFFICE FOR THE PROTECTION OF PERSONAL DATA, establishing that the data importer or the exporter has failed to comply with the Agreement; or (v) the data exporter, without prejudice to the exercise of any other right held against the data importer, may terminate this Agreement when: judicial administration or the liquidation of the importer have been requested, and such request has not been refused within the deadline in effect pursuant to the applicable law; an order of liquidation is issued or its bankruptcy is declared; an administrator for some of its assets is appointed; the data importer has requested the declaration of a bankruptcy proceeding; or a similar situation arises under any jurisdiction. In the cases foreseen in items (i), (ii), or (iv), the data importer may also proceed to the termination without the need of intervention by the supervisory authority.

c) The parties agree that the termination of this agreement for any cause whatsoever shall not release them from compliance with the obligations and conditions in relation to the processing of the transferred personal data.

**Clause 12 – Obligations upon completion of the Personal Data Processing Services**

The parties agree that, upon completion of the provision of personal data processing services for any reason, the importer and the sub-processor shall, at the discretion of the exporter, either return all the transferred personal data and any copies, or destroy them completely and certify their



destruirlos por completo y certificar esta circunstancia al exportador, a menos que la legislación aplicable al importador le impida devolver o destruir total o parcialmente los datos personales transferidos, verificando que dicho plazo de conservación no sea contrario a los principios de protección de datos personales aplicables, y en caso afirmativo se notificará a la autoridad de control.

destruction to the exporter, unless the legislation applicable to the importer prevents him from returning or destroying the transferred personal data either fully or partially, verifying that such retention period is not contrary to the applicable personal data protection principles, and if it is the supervisory authority shall be notified.



## ANNEX A

### DESCRIPTION OF THE TRANSFER

#### ANEXO A DESCRIPCIÓN DE LA TRANSFERENCIA

##### Exportador de datos

"Exportador de datos" significará "Comprador" (tal como se define en el acuerdo principal al que se incorporan estas Cláusulas Modelo Argentina por referencia a través del Anexo de Protección de Información Personal (el "Acuerdo")).

##### Importador de datos

"Importador de datos" significará "Proveedor" (tal como se define en el Acuerdo),

##### Titulares de los datos

"Titulares de los datos" quiere decir "Comprador" y sus afiliados, según corresponda (según se define en el Acuerdo).

##### Características de los datos

"Datos" significará la Información Personal (según se describe en el Acuerdo y Ámbitos de Trabajo y / o Órdenes de Trabajo asociados) que el Proveedor haya recibido o al que haya accedido del Comprador y / o sus afiliados, según corresponda, sus empleados, representantes y contratistas, u otros en nombre del Comprador o sus afiliados.

##### Tratamientos previstos y finalidad

Los datos se procesarán de acuerdo con los términos del Acuerdo y las Declaraciones de trabajo y / o Órdenes de trabajo relacionadas, los cuales establecen el propósito, el contenido, la duración y la naturaleza del Tratamiento.

#### ANNEX A DESCRIPTION OF THE TRANSFER

##### Data exporter

"Data exporter" shall mean "Buyer" (as defined in the main agreement to which these Argentina Model Clauses are incorporated by reference through the Protection of Personal Information Exhibit (the "Agreement")).

##### Data importer

"Data importer" shall mean "Supplier" (as defined in the Agreement),

##### Data owners

"Data owner" shall mean "Buyer" and its affiliates, as applicable (as defined in the Agreement).

##### Characteristics of the data

"Data" shall mean the Personal Information (as described in the Agreement and associated Scopes of Work and/or Work Orders) that is received or accessed by Supplier from Buyer and/or its affiliates, as applicable, their employees, representatives and contractors, or others on behalf of Buyer or its affiliates.

##### Purpose of the data processing to be conducted:

Data shall be processed in accordance with the terms of the Agreement and the related Statements of Work and/or Work Orders, which set out the purpose, subject matter, duration and nature of the Processing.



### **EXHIBIT C – DATA SAFEGUARDS**

1. Supplier shall maintain an information security program that encompasses administrative, technical, and physical safeguards that meet or exceed the requirements specified in the then-current SISR (as defined in Section 5 of this Exhibit) and applicable industry standards to protect against threats to the unauthorized or accidental destruction, loss, alteration, or use of Buyer information, and/or unauthorized disclosure or access to Buyer information.
2. Supplier personnel who are provided ongoing access to Buyer's facilities and/or network and computing resources shall abide by all applicable Acceptable Use policies and complete the information security training approved by Buyer. For such personnel, Supplier shall conduct background checks and/or other investigations deemed necessary, as appropriate and permitted by applicable law. Supplier personnel with direct, unrestricted access to the Johnson & Johnson Network ("JJNET") shall complete Buyer's information security awareness training upon initial access to JJNET and annually thereafter. Supplier's access or connectivity may be terminated at any time upon violation of Buyer's policies and/or misuse or abuse of Supplier's privileges.
3. If Supplier discovers or is notified of a breach or potential breach of security relating to Buyer information that is not intended for public release, or that would otherwise interrupt or degrade the Services to the Buyer, Supplier shall: (a) notify Buyer within 24 hours of such breach or potential breach; and (b) if Buyer information was in the possession of Supplier at the time of such breach or potential breach, Supplier shall (i) promptly investigate and remediate the effects of the breach or potential breach, and (ii) provide Buyer with satisfactory assurance that such breach or potential breach will not reoccur.
4. No Buyer information shall be sold, assigned, leased or otherwise disposed of to a third party, or commercially exploited, by or on behalf of Supplier or its personnel without Buyer's express written consent. Supplier shall not collect, share, disclose or use any Buyer information except as necessary to perform the services described in the Agreement. Furthermore, Supplier represents and acknowledges that it does not receive, nor is Buyer providing, any such Buyer information in consideration for the provision of the services or otherwise. Supplier additionally represents and warrants that the provision of the Services shall comply with applicable data protection laws.
5. "SISR" means the Johnson & Johnson Supplier Information Security Requirements in effect as of the Effective Date, as revised from time to time by Buyer and made available to Supplier. Supplier shall have 30 days after receipt of a SISR revision to object to any new requirements contained therein that would cause a material increase in Supplier's efforts to comply with such new requirements in connection with an existing Work Order. In such case, Supplier shall notify Buyer of any proposed additional fees for such new requirements, which shall apply only if the parties sign a corresponding change order to the applicable Work Order. Absent the parties signing such change order, Buyer may terminate the Work Order without further liability. If Supplier intends to implement a change to its systems, policies or procedures that would reduce the level of safeguards in place as of the Effective Date, Supplier shall notify Buyer and only implement such change upon Buyer's approval.



## **EXHIBIT D - HEALTH CARE COMPLIANCE PROVISIONS**

1. “Health Care Professional” or “HCP” is defined as (i) any person who is licensed by a province to provide health care services directly or indirectly to patients, such as a physician, a nurse, a pharmacist, a technician, a psychologist, or a lab specialist and/or (ii) any person or organization to whom Buyer markets its products and services that is in a position to influence the selection of the products furnished or purchased, including but not limited to hospitals and health systems, administrators, procurement personnel, group purchasing organizations, pharmacy benefit managers, and business people.
2. Supplier shall, with respect to each HCP engaged under this Agreement or any SOW:
  - 2.1 Ensure that the HCP’s services are provided in compliance with all applicable laws and regulations, including but not limited to laws and regulations pertaining to the promotion of products regulated by Health Canada; laws, regulations and guidance pertaining to anti-kickback and submission of false claims to governmental or private health care payors (collectively, “Health Care Compliance” or “HCC”); provincial and federal laws and regulations relating to the protection of individual and patient privacy; and any other laws and regulations applicable to such services;
  - 2.2 Ensure that HCP’s services are provided in compliance with Buyer’s written policies and procedures of which Supplier is provided notice, including, but not limited to, policies and procedures related to Health Care Compliance and the protection of individual and patient privacy (collectively, “Buyer Policies”). The requirements of this Agreement and any additional policies provided attached to this Agreement or the applicable SOW shall constitute Buyer Policies of which Buyer provides notice to Supplier;
  - 2.3 Execute a written agreement setting forth services and compensation for such services, prior to the HCP providing any services pursuant to this Agreement or the applicable SOW. The parties shall include in each SOW a template agreement that Supplier shall use in engaging such HCPs. Supplier shall ensure that any payments made to HCPs do not exceed fair market value for services provided by the HCP;
  - 2.4 Ensure that each HCP that is a health care practitioner is duly licensed in the province where he or she is currently practicing. If an HCP fails to satisfy this requirement at any time during the term of this Agreement or the applicable SOW Supplier must notify Buyer in writing within 10 days of any such change in status, and upon receipt of such notice, Buyer shall have the right to terminate any applicable SOW;
  - 2.5 Ensure that each HCP is qualified and authorized to provide services as may be agreed to by Supplier and Buyer in any applicable SOW, or required by law or any applicable authority, including, but not limited to, any required ethics or other authorizations from federal, provincial or local government agencies for HCPs who are employees of such agencies;
  - 2.6 Compensate each HCP the fair market value for his/her services, based on services provided, and in a manner that does not take into account the volume or value of any prescriptions, referrals or business generated among the parties; and
  - 2.7 Ensure that each HCP complies with professional and/or employment rules (such as conflicts of interest or ethics policies) established by Supplier or a professional organization or institution with which HCP is affiliated when the provision of services by an HCP is subject to such rules, including, as applicable, obtaining any required approval(s) prior to providing services and making any required reports.
3. In the event that Buyer is charged any fee or penalty because Supplier failed to comply with the requirements set forth in this Exhibit, Supplier agrees to reimburse Buyer for such fees or penalties. Buyer reserves the right to reduce or not pay any invoice in the event that Supplier fails to comply with the requirements set forth in this Exhibit.
4. Supplier shall produce and send to Buyer electronic reports each month in which payments were made or gifts or meals were provided to HCPs by Supplier on behalf of Buyer, listing the following:
  - 4.1 value of any gifts, meals, compensation paid, and/or entertainment provided to HCPs, whether their services were obtained through a written agreement or not;
  - 4.2 nature, purpose and date of payments or other items of value provided; and
  - 4.3 names, addresses, and the Federal or Provincial Tax registration number(s) of HCPs who were paid remuneration for Services relating to Buyer.
- 4.4 Supplier shall report any violations of the compliance obligations set forth in this Agreement to Buyer at the name and address listed in Section 20 (Notices) or through the Vendor & Distributor Hotline at 1-800-556-2496.
- 4.5 Supplier, at its expense, shall ensure that all personnel and subcontractors involved in providing Services attend and participate in training and educational programs reasonably scheduled by Buyer. Supplier, at its expense, agrees to train and periodically provide





refresher training to all its new and current personnel and subcontracted personnel providing Services regarding the compliance obligations set forth in this Agreement, including any Buyer Policies applicable to Services. Supplier shall, upon request, provide Buyer with a record of the training provided and the dates training was attended by any Supplier personnel and subcontractors.



## **EXHIBIT E- PHARMACOVIGILANCE**

### **1. Definitions**

For the purposes of this Appendix, any capitalized terms used but not defined below shall have the meanings ascribed thereto in the Agreement:

- 1.1 **“Adverse Event”** (AE) means any untoward medical occurrence in a patient or a clinical-trial subject administered a medicinal product and which does not necessarily have to have a causal relationship with this treatment. An Adverse Event can therefore be any unfavourable and unintended sign (for example, an abnormal laboratory finding), symptom, or disease temporally associated with the use of a medicinal product, whether or not considered related to this medicinal product.
- 1.2 **“Applicable Law”** means the applicable laws, rules, regulations, guidelines, or orders, including any guidelines or other requirements of any Regulatory Authority regulating or otherwise exercising authority with respect to the Product, and industry guidelines or codes of conduct that may apply to the review and analysis of safety information, the reporting of safety information to Regulatory Authorities and the maintenance of records thereof.
- 1.3 **“Date of First Receipt”** means the date of receipt or coming into possession or control of pharmacovigilance data by either of the Parties to this Agreement or by any of their Affiliates or designees, which contains minimum criteria for reporting as defined by the Applicable Law (i.e., an identifiable subject/patient, identifiable reporter, suspect medicinal product, and event). Date of First Receipt shall be considered as the Regulatory Clock Start Date or Day Zero (as such terms are defined by Regulatory Authority regulations or guidelines) for regulatory reporting and safety data exchange purposes. Criteria for reporting is when the Supplier is first aware of an AE, PQC and / or SS occurring during exposure to a Product and is reportable within 24 hours of Date of First Receipt. Any subsequent (follow-up) information is reportable to Buyer within 24 hours of subsequent receipt date(s) (if applicable).
- 1.4 **“Incomplete Case”** means a case that does not contain minimum criteria for reporting as defined by the Applicable Law (i.e., an identifiable subject/patient, identifiable reporter, suspect medicinal product, and event), but at a minimum contains a suspect medicinal product and a suspect event. Such reports are entered on the safety database as potential cases of value for signal detection purposes.
- 1.5 **“Product”** means any pharmaceutical, biological, devices or Combination Product manufactured and/or packaged for commercial and/or clinical distribution for Buyer where Buyer is the marketing authorization holder in Canada.
- 1.6 **“Product Quality Complaint”** (PQC) means any written, electronic or oral communication that alleges deficiencies related to the identity, quality, durability, reliability, safety, effectiveness or performance of a product after it is released for distribution.
- 1.7 **“Combination Product”** means any products for which Buyer is the marketing authorization holder in Canada that combines a drug/biologic component and a device component and is integrated into a singular product or package/unit.
- 1.8 **“Regulatory Authority”** means any applicable federal, national, regional, state, provincial or local regulatory agencies, departments, bureaus, commissions, councils or other government entities regulating or otherwise exercising authority with respect to the Product in the relevant Territory.
- 1.9 **“Special Situation”** means occurrences or reports that may not contain an adverse event, which must still be collected and reported in order to meet regulatory safety reporting requirements and Buyer policies:
  - a. Overdose of Product
  - b. Pregnancy exposure (maternal and paternal)
  - c. Exposure to the Product from breastfeeding
  - d. Suspected abuse/misuse of the Product
  - e. Inadvertent or accidental exposure to the Product (including occupational exposure)
  - f. Any failure of expected pharmacological or medical device action (i.e. lack of effect) of the Product
  - g. Unexpected therapeutic or clinical benefit from use of the Product
  - h. Medication error (includes potential, intercepted or actual) involving the Product with or without patient/consumer exposure to the Product, (e.g. name confusion) OR that caused an unintended effect or could cause an intended effect (e.g. adult medicine given to a young child)
  - i. Suspected transmission of an infectious agent via Product
  - j. Expired drug use and falsified medicine



- k. Off-label use - situations where the Product is intentionally used for a medical purpose not in accordance with the authorized product information

Off-label use without an associated AE, Special Situation, UE, ADE or AEPQC should be collected only when it is specifically and voluntarily brought to the attention of the Supplier in an unsolicited manner by a reporter e.g., Health Care Professional or data obtained from databases where off-label use may be systematically collected (e.g., reimbursement database in Canada), and in accordance with local procedure in compliance with local laws and regulations. Follow-up of off-label use is not required.

1.10 “**Territory**” means Canada.

1.11 “**Undesirable Effect**” (UE) shall mean an adverse reaction for human health attributable to the normal or reasonably foreseeable use of a cosmetic product.

## 2. Reporting Requirements

Supplier shall collect any information in or coming into its possession or control, relating to an AE, special situations (including but not limited to reports of exposure during pregnancy (maternal and/or paternal), breastfeeding; overdose; abuse and misuse; medication errors; suspected transmission of any infectious agents; outside of label use; occupational exposure, inadvertent or accidental exposure; failure of expected pharmacological action, unexpected therapeutic or clinical benefit, expired drug use and falsified medicine), adverse events associated with a PQC for the Product, regardless of source and Incomplete Cases.

Supplier shall collect any information in or coming into its possession or control for the Product regardless of source, relating to an AE, Special Situation, AE associated with a Product Quality Complaint (AEPQC), UE or ADE, as applicable and Incomplete Cases, in a format as agreed upon by the Parties.

Supplier shall forward to Buyer such information immediately, but in no case later than twenty-four (24) hours from the Date of First Receipt by the Supplier. For the avoidance of doubt, all Incomplete Cases should also be collected and forwarded immediately, but in no case later than 24 hours from the date of collection by the Supplier.

## 3. Training

Supplier shall ensure that its personnel involved in the execution of services pertaining to this Agreement (including applicable subcontractors) are trained in the collection and reporting of AEs, Special Situations, AEPQC, UEs or ADEs, prior to the start of the applicable work order and/or project and at least annually thereafter if such services remain in effect, to ensure compliance with this Agreement and the Applicable Law. This includes, but is not limited to, monitoring applicable AE, Special Situation, AEPQC, UE and ADE, training, and maintaining documentation. Buyer may require Supplier to provide additional training to its personnel when there is a change in the governing contracts and/or processes or changes in Supplier personnel. Initial and subsequent annual trainings will be assigned by Buyer, either via Buyer’s Learning Management System or other methods of communication. Upon receipt of the training request, training must be completed by all personnel associated with this Agreement within 28 calendar days. All training records (outside of Buyer’s Learning Management System) must be returned to Buyer within 28 calendar days from the date the training request was received. Copies of training records must be kept on site by the Supplier for audit purposes. Supplier shall inform Buyer of all new personnel that will be associated or providing services under this Agreement so that training can be assigned prior to the provision of services. Supplier shall retain a list of all personnel names that are involved in Pharmacovigilance activities with Buyer. This list should be kept up to date at all times and be readily available upon request from Buyer.

## 4. Establishment of a Tracking System

Supplier shall establish and maintain a tracking system for the collection, recording and collation of safety information for the Product. Supplier must provide a summary of all identified AE, Special Situation, AEPQC, UE and ADE reports, as applicable, as outlined in the Service Provider training and/ or this Agreement, including project protocol, scope of work, or work order. The frequency of reconciliation must be agreed prior to start of the services and will depend on the duration and extent of the services. Supplier and Buyer will collaborate to identify any missing safety information, including, but not limited to, completeness of case identification numbers, in case of discrepancies

## 5. Retention Policy

Supplier shall maintain and archive records of all source documentation generated by the activity (records, questionnaires, reports), personnel training records and other relevant information relating to this agreement, including all project protocol, scope of work and work orders and the Supplier’s obligations under this Agreement for a period specified by Buyer and Applicable Law. Supplier must have appropriate storage capabilities (e.g., preventing accidental damage of physical records



and appropriate back up of electronic storage systems) if storing original AE, Special Situations, AEPQC, UE and ADE documentation. Notwithstanding the above, before Supplier destroys any safety records it will notify Buyer of its intention to do so, affording Buyer the opportunity to retain such records if it so wishes.

## **6. Audit**

Buyer or its designee shall have the right to audit Supplier, to verify compliance with this Agreement and the Applicable Law, provided that Buyer provides Supplier with at least ninety (90) Calendar Days prior written notice. Buyer will review the scope of the audit with the Service Provider; a written audit plan will follow and be submitted by Buyer to the Service Provider within thirty (30) Calendar Days prior to the audit. Supplier will allow access to its facilities, systems, personnel and records such including but not limited to documented AE processes, organization charts, including outlined responsibilities for the personal involved in Pharmacovigilance activities with Buyer as well as applicable backup plan, contractual agreement between Supplier and Buyer, evidences for AE tracking of any initial and subsequent information along with receipt of acknowledgement (unique identifier) of AE cases and evidences for submission of follow-up information and/or reconciliation data upon request from Buyer. The access to Buyer or its designee to facilities, systems, personal and records will be allowed in whatever form and in any location (including locations owned or operated by a third party) as may reasonably be necessary to enable the Buyer or its designee to evaluate and ensure compliance with this Agreement and the Applicable Law. Buyer shall communicate audit findings in a written audit report in a timely manner. The Parties undertake to cooperate with each other to diligently investigate and resolve any such audit findings

## **7. Data Privacy**

In the performance of the pharmacovigilance activities under this Appendix, both Parties will comply with all Applicable Laws with respect to privacy and protection of personal information.

Each Party shall collect, use and disclose any personal data obtained in the course of performing the pharmacovigilance activities under this Appendix solely for the purposes of complying with the regulatory obligations as described in this Appendix, or as otherwise required by Applicable Law or by a court order. Both Parties will use electronic, physical and any other safeguards appropriate to the nature of the information to prevent any use or disclosure of personal data other than as provided for by this Appendix. Both Parties will also take reasonable precautions to protect the personal data from accidental, unauthorised, or unlawful alteration or destruction.

Each Party shall notify the other Party promptly of any accidental, unauthorised, unlawful destruction, loss, alteration, or disclosure of, or access to the personal data, and take immediate steps to rectify any such Security Breach

## **8. Follow Up**

Supplier will be responsible and shall cooperate with Buyer, to diligently follow up on pharmacovigilance data or Incomplete Cases. Follow-up information will follow the same timelines and mechanism as initial information noted above and will include the receipt date for the follow-up information.

## **9. Miscellaneous**

Notwithstanding the above, in the event Supplier is informed of AE, Special Situations and/or PQC, related to the use any other Buyer medicinal products or other Buyer medicinal products that Supplier is aware of, Supplier must report to Buyer within twenty-four (24) hours of Supplier's Date of First Receipt.

Supplier shall perform the pharmacovigilance obligations set out in this Appendix in accordance with Buyer's standard operating procedures.

Buyer and Supplier undertake to notify each other and the EU Qualified Person for Pharmacovigilance immediately of all safety-related regulatory queries from regulatory authorities and ethics committees and all other pertinent interactions with regulatory authorities that relates to the Products or any regulatory action or pending actions within the Territory that might result in a change of labelling or market restriction due to signals, including but not limited to the following:

- 9.1 Marketing authorization withdrawal or suspension;
- 9.2 Failure to obtain a marketing authorization renewal;
- 9.3 Restrictions on distribution;
- 9.4 Clinical trial suspension;
- 9.5 Dosage modification for safety reasons;



- 9.6 Changes in target population or indications for safety reasons; and
- 9.7 Formulation changes for safety reasons.

## 10. Contact Details

For **Buyer:**

For **Supplier:**



## EXHIBIT F - VULNERABILITY SCANNING REQUIREMENTS

If, in performing Services, Supplier is creating or hosting a website for Buyer, then, without limiting Supplier's other obligations under the Agreement, Supplier shall comply with the vulnerability scanning and related requirements set forth in this Exhibit.

For purposes of this Exhibit, the term "**Software**" means any Supplier hosted Internet-facing web site or web application that presents, transmits or processes Buyer's confidential information.

1. **Pre-Production Environment.** Before any Software is released into a production environment, Supplier shall (a) scan such Software for the Open Web Application Security Project current ten most common web applicable security risks ("**OWASP Top 10**") located at [www.owasp.org](http://www.owasp.org) using an industry standard vulnerability scanning tool; (b) remediate, as necessary, any identified vulnerabilities; and (c) transmit to Buyer in a secure manner a written report at least 5 business days prior to production release indicating that no such vulnerabilities or risks exist. To the extent the Software contains any software code provided by or through a third party ("**Third Party Software**"), the term Software as used in this Exhibit shall be deemed to include such Third Party Software. Supplier shall ensure that such Third Party Software satisfies the requirements set forth in this Exhibit. Further, all obligations with respect to the Software set forth in this Exhibit shall include any error correction, bug fix, patch, enhancement, update, upgrade, new version, release, revision or other modification to the Software provided or made available by Supplier pursuant to the Agreement, including without limitation, the provision of maintenance, support or other services.
2. **Production Environment.**
  - a. Once the Software is released into a production environment, Supplier shall (i) scan such Software for the OWASP Top 10 within 24 hours of "going live" and every 90 days thereafter using an industry standard vulnerability scanning tool; and (ii) transmit to Client in a secure manner a written report within 5 business days of each scan that includes the summary results of such scan.
  - b. Supplier shall remediate all vulnerabilities in the Software at Supplier's expense and in a timeframe commensurate with the risk, as set forth below, which requirements Supplier shall have the right to amend from time to time. Without limiting Buyer's other remedies under the Agreement and at law, in the event of any failure of Supplier to remediate any vulnerability in accordance with the requirements set forth herein (as may be amended from time to time), Buyer may immediately terminate the Agreement and/or applicable order for cause.
    - i. "**High Risk**" means any vulnerability identified by the scanning tool as being a high risk or a critical flaw that could allow for exploitation of the Software. Supplier shall remediate each High Risk finding within 30 days of identification. Further, upon request from Buyer, Supplier shall immediately remove or disallow access to the website or webpage affected by such High Risk finding temporarily until such finding is remediated in accordance with this Exhibit.
    - ii. "**Medium Risk**" means any vulnerability identified by the scanning tool as being a medium risk or a significant flaw that presents the potential for exploitation of the Software. Supplier shall remediate each Medium Risk finding within 60 days of identification.
    - iii. "**Low Risk**" means any vulnerability identified by the scanning tool as being a low risk or a flaw that presents the potential for exploitation of the Software. Supplier shall remediate each Low Risk finding in accordance with its internal policies and procedures.
  - c. Without limiting the foregoing periodic scanning obligations, Supplier shall, at all times once the Software has been released into a production environment, implement and maintain appropriate controls to identify any vulnerabilities in the Software. Supplier shall notify Buyer in writing: (i) of any publicly acknowledged vulnerabilities or "0 day exploits" immediately upon such public acknowledgement; and (ii) of internally-known, yet publicly undisclosed vulnerabilities or "0 day exploits" within 5 business days of their discovery. Supplier shall remediate each such vulnerability or "0 day exploit" within 5 days, or a timeframe agreed to by Buyer.
3. **Buyer's Rights.** Notwithstanding Supplier's obligations as set forth in this Exhibit, Buyer may perform or cause a third party to perform vulnerability scanning, penetration testing and/or other related activities with respect to the Software and services provided by Supplier under the Agreement, which Buyer may do in its sole discretion with or without notice to Supplier.



## **EXHIBIT G RECORDS AND INFORMATION MANAGEMENT (“RIM”) REQUIREMENTS**

1. **Buyer’s Records and Information.** All records and information, in any format, that Supplier creates, edits or receives on behalf of Buyer or Buyer’s affiliates will be referred to herein as “Buyer’s Records and Information.” For avoidance of doubt, “Buyer’s Records and Information” does not include records and information created by Supplier as part of Supplier’s business processes (e.g., invoices, internal reports, etc.).
  - 1.1 Supplier shall maintain, manage and protect Buyer’s Records and Information pursuant to this Agreement and any applicable Statement of Work or Work Orders (i) in accordance with Buyer’s records retention requirements; and (ii) in accordance with all applicable statutes and regulations.
  - 1.2 Supplier shall not transfer Buyer’s Records and Information to any other entity unless directed by Buyer.
  - 1.3 Supplier shall manage Buyer’s Records and Information such that Buyer’s Records and Information is not intermingled with records and information managed by Supplier for other customers.
  - 1.4 Supplier shall retain electronic data backups of Buyer’s Records and Information for disaster recovery, record retention requirements, or delivery of Services.
2. **Preservation and Production.** Supplier shall comply with any request from Buyer to preserve Buyer’s Records and Information (or parts thereof). Supplier shall deliver promptly Buyer’s Records and Information requested to be searched, retrieved, and produced, all as part of the services Supplier provides under this Agreement and any applicable Statement of Work or Work Orders in accordance with Section 8. (Format of Buyer’s Records and Information).
3. **Third Party Requests.** Within three business days of Supplier receiving from anyone other than Buyer a request, demand, notice, subpoena, order, or other legal request (“**Third-Party Request**”) for Buyer’s Records and Information, Supplier shall notify Buyer and provide Buyer with a copy of the Third-Party Request (unless legally prohibited). Supplier shall confer with Buyer to identify, document, and implement procedures to comply with the request. Supplier shall take all reasonable steps to protect Buyer’s legal rights when responding to a Third-Party Request.
4. **Training.** All employees and contractors of Supplier with access to the Johnson & Johnson Enterprise Network (JJNET) shall annually complete Records and Information Management training as specified by Buyer.
5. **Destruction.** Supplier shall not destroy or permanently delete Buyer’s Records and Information without Buyer’s written approval. Buyer shall confirm the Buyer’s Records and Information is not subject to any pending preservation obligation or retention requirement. Supplier shall certify in writing that Buyer’s Record’s and Information has been destroyed or permanently deleted as specified by the Buyer.
6. **Transfer.** When a transfer of Buyer’s Records and Information from Supplier is required, Supplier shall (i) transfer Buyer’s Records and Information to Buyer or an entity specified by Buyer in accordance with Section 8. (Format of Buyer’s Records and Information), (ii) take no action on Buyer’s Records and Information until written notification from Buyer confirming accurate and complete transfer is received, and (iii) obtain Buyer’s written approval to destroy or permanently delete Buyer’s Records and Information in accordance with Section 5. (Destruction).
7. **Termination.** Upon termination of this Agreement and any applicable Statement of Work or Work Order and at Buyer’s direction, Supplier shall (i) transfer Buyer’s Records and Information to Buyer or an entity specified by Buyer in accordance with Section 6. (Transfer), or (ii) obtain Buyer’s written approval to destroy or permanently delete Buyer’s Records and Information in accordance with Section 5. (Destruction).
8. **Format of Buyer’s Records and Information.** In consultation with Buyer, Supplier shall identify Buyer’s Records and Information and implement documented procedures to deliver to Buyer or an entity specified by Buyer, Buyer’s Records and Information and supporting documentation in the format directed by Buyer. To meet Buyer’s records retention and other legal preservation obligations, Buyer may require Supplier to provide Buyer’s Records and Information in a structured format maintaining the relationships that exist in the database underlying Supplier’s application.





## **EXHIBIT H - SOFTWARE AS A SERVICE EXHIBIT**

This Exhibit to the Services Agreement shall apply to any and all SaaS Services (as hereinafter defined) and related services provided by Supplier to Buyer in connection with the Services described in the Agreement.

1. **DEFINITIONS.** Defined terms have the meanings set forth in this Section (Definitions) and elsewhere in this Exhibit, and the Agreement, when capitalized, and may be read in singular, plural or an alternative tense as the context requires.
- 1.1. **“Buyer Data”** means (a) all data, information, content and other materials pertaining to any and all users of the SaaS Services and (b) all data, information, content and other materials emanating from the use of, concerning or contained in, or otherwise transmitted by or through, the Services or otherwise provided by Buyer.
- 1.2. **“Destructive Elements”** means computer code, programs or programming devices that are intentionally designed to disrupt, modify, access, delete, damage, deactivate, disable, harm or otherwise impede in any manner, including aesthetic disruptions or distortions, the operation of the Services or any other associated software, firmware, hardware, computer system or network or any other harmful, malicious or hidden procedures, routines or mechanisms that would cause such SaaS Services to cease functioning or to damage or corrupt data, storage media, programs, equipment or communications, or otherwise interfere with operations.
- 1.3. **“Documentation”** means the manuals, specifications and other written and/or electronic materials describing the functionality, features, security and operating characteristics, maintenance, operation and use of the Services, together with any updates thereto, as provided by or through Supplier to Buyer in accordance with this Exhibit.
- 1.4. **“Error”** means (a) any failure of the SaaS Services, or any portion thereof, to: (i) comply with all applicable laws, (ii) meet or exceed the Functional Specifications, (iii) function and perform in conformance with the Documentation, or (b) any other occurrence or omission that renders the SaaS Services unavailable for use or deficient in operation.
- 1.5. **“Functional Specifications”** means the features, functionality, configuration and other specifications and requirements for the SaaS Services that are: (a) identified in any SOW; (b) published by Supplier; or (c) set forth in the Documentation.
- 1.6. **“SaaS Services”** means the Software and related software-as-a-service, hosting, maintenance and/or support services made available by Supplier for remote access and use by Buyer and its affiliates, including any Documentation and updates thereto and any equipment or technology used by Supplier in connection with the foregoing. The SaaS Services shall be deemed Services (as defined in the Agreement).
- 1.7. **“SaaS Services Fee(s)”** means any and all charges due for the SaaS Services as set forth in the applicable SOW.
- 1.8. **“Software”** means the object code version of Supplier's computer software, the Documentation and all updates made available by Supplier to Buyer under this Exhibit.

## **2. SAAS SERVICES.**

- 2.1. **SaaS Services.** Supplier grants to Buyer a worldwide, non-exclusive, non-transferable right and license to access and use, and to permit users to access and use, the SaaS Services. Supplier shall provide the SaaS Services in accordance with Attachment A (SaaS Services Attachment) and as otherwise set forth in this Exhibit and the applicable SOW. Buyer may make a reasonable number of backup or archive copies of the Documentation at no additional charge. Supplier grants to Buyer the right to permit its affiliates or one or more third parties to exercise any or all of the rights and licenses granted to Buyer hereunder; *provided, however*, that, in the case of third parties, any such third party shall exercise such rights solely to provide goods to or perform services for Buyer and its affiliates. Except as otherwise set forth in the Agreement, or this Exhibit, Supplier and its licensors own and shall retain all right, title, and interest, including, without limitation, all intellectual property rights, in and to the SaaS Services and related deliverables. Buyer shall have only those rights as are expressly granted to it pursuant to the Agreement. If Supplier believes that Buyer or its affiliates have exceeded their rights under this Exhibit through increased usage, and Buyer does not contest such allegation, or it is ultimately determined that such belief was correct, Supplier's sole and exclusive remedy is to invoice Buyer proportionally for such increased usage using the rates set forth in the SOW, including any discounts contained therein, unless Buyer promptly eliminates such increased usage.
- 2.2. **Buyer Data.** Buyer owns and shall retain all right, title, and interest, including, without limitation, all Intellectual Property Rights, in and to the Buyer Data. Supplier has only those rights in and to the Buyer Data as are expressly granted to it pursuant to this Exhibit. Buyer hereby grants to Supplier a worldwide, non-exclusive, nontransferable right and license to store, host, reproduce, maintain, process and transmit the Buyer Data solely for the provision of the SaaS Services in accordance with this Exhibit. Supplier shall protect Buyer Data in accordance with all provisions of applicable laws relating to Buyer Data and the privacy and security thereof, and with Buyer's policies and instructions. Supplier shall, upon request by Buyer and at no additional charge, provide Buyer a complete and current copy of Buyer Data in the format requested by Buyer.



### 3. ACCEPTANCE TESTING.

Following Buyer's successful access to the SaaS Services, Buyer shall have 180 days to test the SaaS Services (the "**Acceptance Test**") to determine, in its reasonable discretion, whether it materially conforms to: (a) the Documentation and Functional Specifications; and (b) any other test criteria agreed to by the parties. Supplier shall assist Buyer in the performance of such Acceptance Test. Buyer shall notify Supplier in writing within 10 days after expiration of the Acceptance Test indicating acceptance (the date of such acceptance, the "**Acceptance Date**") or rejection of the SaaS Services, and any non-conformities contained therein. Upon receipt of a rejection notice, Supplier shall have 30 days to remedy the non-conformance. Upon receipt of the revised SaaS Services, Buyer may perform additional Acceptance Tests for the longer of: (a) 30 days; or (b) the time remaining on the original 180 day Acceptance Test period. If Buyer rejects any SaaS Services, Buyer may: (a) immediately terminate the SaaS Services without further payment obligation or liability of any kind, whereupon Supplier shall promptly refund to Buyer, within 10 days, all amounts paid by Buyer under the applicable SOW in connection with such SaaS Services; or (b) require that Supplier correct the deficiencies disclosed by the Acceptance Test and repeat such Acceptance Test until successfully completed, reserving the right to terminate at any time.

### 4. SAAS SERVICES FEES.

Buyer shall pay Supplier all applicable SaaS Services Fee(s) as set forth in the applicable SOW. Unless otherwise expressly set forth in the applicable SOW: (a) the Fees are inclusive of all charges relating to the SaaS Services listed on the applicable SOW; (b) all Fees will be invoiced and payable in U.S. Dollars; and (c) Supplier is solely responsible for all expenses incurred by or on behalf of Supplier, including its personnel and permitted subcontractors, in connection with the Agreement. If Buyer renews the SaaS Services, any SaaS Services Fee(s) increase shall not: (a) occur more than once in any 12 month period; or (b) exceed the lesser of: (i) the percentage increase in the Consumer Price Index for All Urban Consumers for the previous 12 months, as published by the United States Department of Labor; or (ii) 3% of the then-current SaaS Services Fee(s).

### 5. REPRESENTATIONS AND WARRANTIES; ERROR CORRECTION.

- 5.1. Representations and Warranties. Supplier represents and warrants that: (a) the SaaS Services will conform in all material respects with the applicable Functional Specifications; (b) Supplier is in compliance with its responses to any vendor security risk assessment, privacy or other vendor assessment that Buyer may conduct and will notify Buyer promptly of any changes that might result in non-compliance with such responses; (c) Supplier has the right to grant the license and other rights relating to any Services provided under and during the term of this Agreement and shall maintain all rights in and to the Services necessary to permit Buyer to exercise the licenses and other rights granted hereunder; and (d) the SaaS Services do not and will not contain any Destructive Elements. Notwithstanding anything contained herein to the contrary, if the SaaS Services contain any Destructive Elements, Supplier will be deemed to be in breach of the Agreement and no cure period shall apply.
- 5.2. Error Correction. Supplier shall correct any Errors in the SaaS Services at Supplier's expense during the term of the applicable SOW in accordance with Attachment A (SaaS Services Attachment). If the SaaS Services do not perform as warranted, Supplier will promptly and in accordance with Attachment A (SaaS Services Attachment), correct, replace or modify the SaaS Services at Supplier's expense, so as to provide Buyer with SaaS Services that perform as warranted. If after correction, replacement or modification, the SaaS Services fail to perform as warranted, Supplier, at Buyer's option, shall (x) promptly refund all amounts paid by Buyer under the applicable SOW, or (y) continue to correct, replace or modify the SaaS Services in accordance with Attachment A (SaaS Services Attachment) such that the SaaS Services perform as warranted.

### 6. TERM AND TERMINATION.

- 6.1. Term of SaaS Services. The initial term of the SaaS Services shall be coterminous with the Agreement unless otherwise set forth in the applicable SOW. At the conclusion of the initial SaaS Services Term, Buyer, at its option, may extend the term of the SaaS Services for additional term(s) (each initial term and any renewal term, individually and collectively, the "**SaaS Services Term**") upon the same terms and conditions as set forth herein. Not less than 6 months prior to the expiration of the then-current SaaS Services Term, Supplier shall notify Buyer in writing of Buyer's right to renew the SaaS Services for an additional SaaS Services Term, including the applicable SaaS Services Fee(s), consistent with this Exhibit. In the absence of such SaaS Services renewal notice, Buyer may renew the SaaS Services at the same price as the then-current SaaS Services Term. At any time during the SaaS Services Term and upon 30 days' prior written notice to Supplier, Buyer may: (a) upgrade the SaaS Services to a level of services similar to but higher than the SaaS Services, provided such higher level of services are generally available to Supplier's other customers; or (b) downgrade the SaaS Services to a level of services lower than the SaaS Services, provided such lower level of services are generally available to Supplier's other customers, with any unused, prepaid SaaS Services Fee(s) being credited toward such other SaaS Services.

- 6.2. Termination for Cause. Subject to Section 2.3 (Termination of SOWs for Cause) of the Agreement, if Buyer terminates the SaaS Services, in whole or in part, for cause, Supplier shall promptly refund to Buyer an amount equal to the unused portion of the SaaS Services Fee(s) paid hereunder, corresponding to the length of time remaining in the then-current SaaS Services Term.
- 6.3. Termination for Convenience. Buyer may terminate any incomplete SOW for SaaS Services to which it is a party, any SaaS Services provided to Buyer under a SOW, or the license to one or more modules or features of the SaaS Services licensed under a SOW, in whole or in part, at any time, for any reason or no reason, effective upon no less than 10 days' prior written notice to Supplier, without any further obligation, liability or damage; *provided, however*, that Buyer remains responsible for the payment of any SaaS Services Fee(s) due and owing prior to the applicable effective date of termination. If Buyer terminates any SaaS Services for convenience: (a) Supplier shall be entitled to a pro rata payment for any terminated SaaS Services in progress based on the percentage of work Supplier has completed as of the date Supplier receives such notice of termination and (b) Buyer will have no obligation to pay any other SaaS Services Fee(s) with respect to such terminated SaaS Services.

**7. PRIORITY.**

Notwithstanding anything to the contrary in the Agreement, and solely with respect to the SaaS Services, in the event of any conflict between any terms or conditions contained in this Exhibit, the Agreement, or any attachment to this Exhibit, the following agreements and documents shall control in the following order of descending precedence: (a) this Exhibit, (b) an attachment to this Exhibit, (c) the Agreement, and (d) the applicable SOW. Notwithstanding the foregoing, provisions of this Exhibit and the Agreement may be modified in a change order, solely for the purposes of that change order, only by an express statement specifically identifying the relevant provision of this Exhibit or Agreement to be modified.

**8. SURVIVAL.**

The following Sections of this Exhibit survive any termination or expiration of this Exhibit or the Agreement and any termination or completion of any or all SOWs: (Definitions), (SaaS Services), (Audit), 6 (Representations and Warranties); 6 (Term and Termination), 7 (Priority), 9 (Survival) and any other provisions that by their nature and context are intended to survive.



## Attachment A (SaaS Services Attachment)

1. **Hosting and Data Residency.** Supplier shall provide: (a) all infrastructure, software and services necessary to host, operate, maintain and manage the SaaS Services, and provide Buyer continuous access thereto, in accordance with the terms and conditions set forth in this SaaS Services Exhibit, any applicable SOW and the Agreement; and (b) Buyer shall be entitled to unlimited storage in connection with the SaaS Services during the term of this Agreement.
2. **Backups.** Supplier shall at its sole expense: complete backup copies of the Buyer Data daily (with a complete replication of Buyer Data every 4 hours) and shall safeguard and securely store such copies within the United States. At any time as reasonably requested by Buyer, Supplier shall at its expense promptly deliver to Buyer a complete electronic copy of the then-current version of the Buyer Data, including all electronic documents and related data, in a mutually agreed upon format.
3. **Technical Support.** Supplier shall establish, sufficiently staff and maintain the organization and processes necessary to provide telephone, email and web-based technical support, troubleshooting, SLA Incident(s) identification, isolation, response and remediation, and other assistance in accordance with Annex 1. The contact information for Supplier's technical support organization is set forth in Annex 1. Supplier shall appoint a Technical Account Manager ("**TAM**"). The TAM shall provide Buyer with technical guidance and expertise, will be responsible for participating on Priority 1 SLA Incident(s) troubleshooting conference calls, as requested by Buyer, and will serve as Buyer's single point of contact for escalations.
4. **Browsers.** Supplier shall provide all SaaS Services, including all features and functionality, in compliance with HTML5 standards and compatible with the four browsers with leading market share.
5. **Availability.** For each "**Reporting Period**" (as set forth in Annex 1), the SaaS Services will have a minimum availability service level of 99.95%, excluding "**Scheduled Downtime**," as set forth in Annex 1 ("**Minimum Availability Level**"). Supplier shall notify Buyer in writing of the duration and timing of any Scheduled Downtime, at least 5 business days in advance.
6. **Incident Response and Resolution.** If Supplier becomes aware of a Priority 1, or Priority 2, SLA Incident(s) (as set forth in Annex 1), Supplier shall notify Buyer promptly, but in any event within the applicable "Initial Response" period (as set forth in Annex 1), and such notice will identify the SLA Incident(s) Priority Level based on Supplier's initial evaluation. Supplier and Buyer shall cooperate in good faith to jointly determine the SLA Incident(s) Priority Level; *provided, however*, if Supplier and Buyer cannot reach a joint determination despite such good faith cooperation, Buyer's determination will control. Buyer may report to Supplier any SLA Incident(s) 24 hours per day, seven days per week. Upon notification by Buyer of an SLA Incident(s), Supplier shall promptly commence, and diligently pursue, correction of such SLA Incident(s) at all times and instances employing (a) the "Level of Effort" set forth in Annex 1, and (b) providing an "Initial Response," "Preventive Action," "Root Cause Analysis Report" (as defined below), "Service Restoration" and "Status Update(s)" (as defined below) in accordance with Annex 1. The timeframes for Supplier's responses shall be measured from the earlier of the time that Buyer notifies Supplier, or Supplier first becomes aware of the relevant SLA Incident(s). Supplier shall provide Buyer with updates to the status of Supplier's efforts ("**Status Update(s)**") by telephone, email or such other means as may be reasonably designated by Buyer from time to time, no less frequently than the timeframes set forth in Annex 1.
7. **Reports.** Supplier shall provide Buyer:
  - a) with reports as mutually agreed in writing, specifying in reasonable detail Supplier's performance in relation to availability of the SaaS Services and the service levels set forth in Annex 1 ("**Service Levels**"). If Supplier fails to meet such Service Levels, Supplier shall provide Buyer with a specific plan of action to remedy any SLA Incident(s) and Supplier's performance deficiency.
  - b) with a Supplier-prepared, written "**Root Cause Analysis Report**" (or "**RCA Report**"), in the form of an executive summary, including supporting technical details at Buyer's request, which documents the relevant SLA Incident(s) and contains a detailed description of the SLA Incident(s), the action(s) taken to restore the SaaS Services and/or resolve the SLA Incident(s), the root cause of the SLA Incident(s) and an action plan to ensure such SLA Incident(s) will not re-occur.
8. **Service Credits.** Supplier's failure to meet the Service Levels entitles Buyer to "**Service Credits**" (as set forth in Annex 2) based on the SaaS Services Fees that would otherwise be payable for the SaaS Services Term in which such failure occurs. Any Service Credits owed to Buyer hereunder will, at Buyer's option, be: (a) refunded by Supplier to Buyer within 30 days of the date such Service Credits accrued, or (b) offset against subsequent Service Fees owed by Buyer. Supplier agrees that the payment, or offset, of any Service Credits will not relieve Supplier of any of its obligations under the Agreement, or otherwise limit Supplier's liability for any breach thereof, including without limitation, any Buyer remedies pursuant to Section 9 (Excessive Performance Failure).
9. **Excessive Performance Failure.** Following an Excessive Performance Failure (as defined below), upon written notice to Supplier, Buyer may immediately terminate the applicable SOW or Agreement (in Buyer's sole discretion) without further payment obligation, or liability to Supplier (other than for payment of undisputed SaaS Services Fee(s) due and owing as of the effective date of termination). An Excessive Performance Failure will be deemed to be a breach of a material term of the Agreement, which shall not be subject to cure. "**Excessive Performance Failure**" means (a) failure to meet defined availability Service Levels for two Reporting Periods in a 12-month period, or (b) failure to meet an availability level of 98% in any calendar month.



## Annex 1 to Attachment A

### Service Level Details

SLA Incident(s) Priority	Definition of SLA Incident(s)	Level of Effort	Initial Response	Service Restoration	RCA Report	Preventive Action	Status Updates
1	Any incident in a production environment that (i) renders the SaaS Services or any material functionality therein inoperative (incl. impaired Buyer use, data loss/corruption); (ii) causes the mean SaaS Services response time to exceed 10 seconds; or (iii) results in unavailability of the Supplier's API (where applicable).	Continuous best efforts, 24 hours per day, 7 days per week	Immediate, but in no event to exceed 30 minutes	Four hours	10 calendar days	30 calendar days	Every hour until a Service Restoration is provided and every calendar day thereafter until a Preventive Action is provided.
2	Any incident (i) that materially adversely affects the functionality of the SaaS Services, causes a material portion of the SaaS Services' functionality to be unavailable, causes the mean SaaS Services response time for user access to and from the SaaS Services to exceed 5 seconds; or (ii) in a non-production environment that renders the SaaS Services or any material functionality therein inoperative (incl. an SLA Incident(s) that materially impairs Buyer's use of the SaaS Services or causes Buyer to experience data loss or corruption or causes an essential part of the SaaS Services to be unusable).	Continuous best efforts, 24 hours per day, 7 days per week	One hour	Eight hours	10 calendar days	30 calendar days	Every two hours until a Service Restoration is provided and every calendar day thereafter until a Preventive Action is provided.
3	Any incident that (i) has a minor impact; or (ii) in a non-production environment that materially adversely affects the functionality of the SaaS Services or causes a material portion of the SaaS Services functionality to be unavailable.	Commercially reasonable efforts, during normal business hours	One Business Day	Three calendar days	N/A	Next update or the update immediately thereafter, as reasonable	N/A
4	Any incident: (i) in a production environment that does not adversely affect Buyer's or any of its Affiliate's business operations; or (ii) in a non-production environment that has a minor impact.	Commercially reasonable efforts, during normal business hours	One Business Day	Eight calendar days	N/A	Next update or the update immediately thereafter, as reasonable	N/A

**"Scheduled Downtime"** means scheduled maintenance of the SaaS Services during a Reporting Period in accordance with this SaaS Services Schedule. The total amount of Scheduled Downtime shall not exceed 60 minutes during any Reporting Period.

**"Reporting Period"** means one calendar month.

[Please insert contact information for Supplier's technical support organization (see Section 3 of this Attachment A).]

## Annex 2 to SaaS Services Attachment

### Service Credits

1. **Availability Services Credits.** The Availability Services Credits are calculated as follows:
  - 1.1 “**Availability Hours**” means 24 hours multiplied by the number of days in the applicable Reporting Period and then deducting from such result any Scheduled Downtime hours occurring in such Reporting Period.
  - 1.2 The “**Availability Services Credit**” for the applicable Reporting Period is calculated in accordance with the following formula:
$$[(\text{Availability Hours} - \text{Unscheduled Downtime}) / \text{Availability Hours}] * 100\%$$

2% of SaaS Services Fee(s) for the applicable Reporting Period for each 1% below the Minimum Availability Level.
2. **SLA Incident(s) Response and Resolution.** The Services Credits for any miss of the timeframes identified in Annex 1, above, are calculated as follows:

SLA Incident(s) Priority	Amount of Service Credits		
	Initial Response	Service Restoration	Preventive Action
1	1/360 <sup>th</sup> of the annual SaaS Services Fee(s) for each additional hour or portion thereof	1/360 <sup>th</sup> of the annual SaaS Services Fee(s) for each additional hour or portion thereof	1/360 <sup>th</sup> of the annual SaaS Services Fee(s) for each Priority 1 Incident in a Reporting Period after the first Priority 1 Incident.
2	1/360 <sup>th</sup> of the annual SaaS Services Fee(s) for each additional hour or portion thereof	1/360 <sup>th</sup> of the annual SaaS Services Fee(s) for each additional 2 hour period or portion thereof	1/360 <sup>th</sup> of the annual SaaS Services Fee(s) for each Priority 2 Incident in a Reporting Period after the first Priority 2 Incident.
3	N/A	1/360 <sup>th</sup> of the annual SaaS Services Fee(s) for each additional Business Day or portion thereof	N/A
4	N/A	1/360 <sup>th</sup> of the annual SaaS Services Fee(s) for each additional Business Day or portion thereof	N/A



# eSignature Request between JJVC div Client Inc and Supplier

Final Audit Report

2023-03-1

## "eSignature Request between JJVC div Client Inc and Supplier" History

Agreement completed.

2023-03-17 - 7:01:12 PM GMT